FALL 2025

MATH 330: Abstract Algebra

August 22, Friday

Chapter 1 – Preliminaries

- $A = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$
- $B = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$
- Prove $A = B$.

Proof:

- $A \subseteq B$
  - Let $x \in A$.
  - Then $x = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$.
  - If $b > 0$, $b \in \mathbb{N}$, so $x \in B$.
  - If $b < 0$, then let $x = \frac{-a}{-b}$.
  - Now $-a \in \mathbb{Z}$ and $-b > 0$ and $-b \in \mathbb{Z}$ so $-a \in \mathbb{Z}$ and $-b \in \mathbb{N}$ so $x \in B$.
  - This shows $A \subseteq B$.
- $B \subseteq A$
  - Let $y \in B$.
  - Then $y = \frac{a}{b}$ with $a \in \mathbb{Z}$ and $b \in \mathbb{N}$.
  - Since $b \in \mathbb{N}$, $b \in \mathbb{Z}$ and $b \neq 0$ so $y \in A$.
  - So $B \subseteq A$.
- Therefore $A = B$. □

---

function: $f: \overset{\text{domain}}{A} \to \overset{\text{codomain}}{B}$ is a function from A to B if for any $a \in A$, $\exists!$ $b \in B$ such that $f(a) = b$.

↗ everyone gets a letter

onto: $f: A \to B$ is onto if $Im(f) = B$

ex: $f(x) = x^3$ when $f: \mathbb{R} \to \mathbb{R}^3$ is onto. but not when $f: \mathbb{Z} \to \mathbb{Z}$ because $f(x) = 2$ doesn't work.

↗ no one gets two letters

one-to-one: $f: A \to B$ is 1-1 if whenever $f(a) = f(b) \iff a = b$.

↗ everyone gets exactly one letter

bijection: $f: A \to B$ is bijective if f is 1-1 and onto

A relation on a set A is a subset of $A \times A$.

A relation "from" A to B is a subset of $A \times B$.

Chapter 2

Induction

Prove $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$

proof:

- $P(1)$ holds since $LHS = 1$, $RHS = \frac{1(1+1)}{2} = 1$
- Suppose $P(n)$ holds s.t. $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.
- Now, show $P(n+1)$ holds s.t. $\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}$
- Notice that $P(n+1) = P(n) + n+1$
$$= \frac{n(n+1)}{2} + n+1$$
$$= \frac{n(n+1) + 2(n+1)}{2}$$
$$= \frac{(n+1)(n+2)}{2} \quad \square$$

Prove that for $n \geq 3$, $2^n > n+4$.

Proof:

- $P(3)$ holds since $2^3 > 3+4$.

Prove that $\forall n \in \mathbb{N}$, $9 \mid 10^{n+1} + 3 \cdot 10^n + 5$.

Proof:

- $P(1)$ holds since $10^2 + 3 \cdot 10^1 + 5 = 135$ and $9 \mid 135$.
- Now, suppose $P(k)$ holds $\forall k = n$ s.t. $9 \mid 10^{k+1} + 3 \cdot 10^k + 5$.
- Now, show $P(k+1)$ holds s.t.: $9 \mid 10^{k+2} + 3 \cdot 10^{k+1} + 5$

  135
  1305 = (135)(10) − 45
  13005 = (1305)(10) − 45
- Notice that $P(k+1) = P(k) \cdot 10 - 45$
$$= (10^{k+1} + 3 \cdot 10^k + 5)\, 10 - 45$$
$$= 9\Big(\underbrace{\frac{10^{k+1} + 3 \cdot 10^k + 5}{9}}_{\text{integer by IH}} \cdot 10 - 5\Big)$$
- Thus $9 \mid 10^{k+2} + 3 \cdot 10^{k+1} + 5$. □

For $n \in \mathbb{N}$ and any $a, b \in \mathbb{R}$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Proof:

- $P(1)$ holds since LHS : $(a+b)^1 = a+b$

  RHS : $\sum_{k=0}^{1} \binom{1}{0} a^0 b^1 + \binom{1}{1} a^1 b^0$

  $= b + a = a+b.$

- Suppose $P(n)$ holds $\forall n \geq 1$ s.t

  $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

- Now, let's show $P(n+1)$ holds s.t

  $(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}$

- Notice that

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n \\ &= (a+b) \sum_{k=0}^{n} \binom{n}{k} a^n b^{n-k} \\ &= a \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} + b \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\ &= \sum_{n=k}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{n=k}^{n} \binom{n}{k} a^k b^{n+1-k}\end{aligned}$$

Division Algorithm

thm:

- For any integers a and b with $b>0$, there exist unique integers q (quotient) and r (remainder) such that:

  $a = bq + r$ where $0 \leq r < b$ → needed for uniqueness

  if $r \geq b$, you can still divide

remark:

- If $a, b \in \mathbb{Z}$, $b \neq 0$, then the statement holds if you write $0 \leq r < |b|$.

proof: smallest counterexample

- Let $S = \{a - bq \in \mathbb{Z} \mid q \in \mathbb{Z}$ and $a - bq \geq 0\}$
- claim: $S \neq \emptyset$
  - case 1: $a \geq 0$, set $q = 0$

    $a - b \cdot 0 = a \in S.$
  - case 2: $a < 0$, set $q = a$

    $a - b \cdot a = a(1-b)$

    since $a < 0$ and $b > 0$, $1 - b \leq 0$ ∴

    $a(1-b) \geq 0 \Rightarrow a - ba \in S$
- By the WOP, S has a smallest element r.
- Then $r = a - bq$ so $a = bq + r$.
- We need to show $r < b$. Suppose FTSOC that $r \geq b$.
- Then $r - b \geq 0 = (a - bq) - b \geq 0$

  $= a - b(q+1) \geq 0$
- This shows that $r - b \in S$ and $r - b < r$. ↯ r is the smallest element of S
- Therefore $r < b$ so $0 \leq r < b$. □

proof: uniqueness

- Suppose q, q' and r, r' are such that

  $a = bq + r = bq' + r'$
- Assume $r' \geq r$.
- Then,

  $bq - bq' = r' - r$

  $b(q - q') = r' - r$
- LHS: multiple of b
- RHS: $0 \leq r' - r < b$ since

  $0 \leq r < b$ and $0 \leq r' < b$

  $\Rightarrow$ LHS = RHS = 0

  $\Rightarrow$ $r = r'$ and $q = q'$ since $b(q - q') = 0$ and $b > 0$.

Euclidean Algorithm

thm:

- Let a, b be positive integers such that $a \geq b$.
- Either $b \mid a$, so $a = bq + 0$ for some $q \in \mathbb{Z}$, or there exists $q_1, q_2, \ldots, q_{n+1}, r_1, r_2, \ldots, r_n$ such that

$$a = bq_1 + r_1 \quad \text{with} \quad 0 < r_1 < b$$
$$b = r_1 q_2 + r_2 \quad \text{with} \quad 0 < r_2 < r_1$$
$$r_1 = r_2 q_3 + r_3 \quad \text{with} \quad 0 < r_3 < r_2$$
$$\vdots$$
$$r_{n-3} = r_{n-2} q_{n-1} + r_n \rightarrow \gcd(a,b)$$
$$r_{n-2} = r_{n-1} q_n + 0$$

$r_0 = b$

- Then $\gcd(a,b) = r_n$.

proof: termination

- Notice that the sequence of remainders $\{r_1, r_2, r_3, \ldots\} \subseteq \mathbb{N}$ and is decreasing.
- By the WOP, it terminates say at $r_n = 0$ for some finite n.

proof: $\gcd(a,b) = r_{n-1}$ (last non-zero remainder)

- We need to show that r_{n-1} is a common divisor of a and b, and the greatest such.
- Let's show it's a common divisor.
- From $r_{n+2} = r_{n+1} q_n + 0$, we get $r_{n-1} \mid r_{n+2}$.
- From $r_{n+3} = r_{n+2} q_{n-1} + r_n$, we get $r_{n-1} \mid r_{n+3}$ since $r_{n+1} \mid r_{n+2}$ and $r_{n+1} \mid r_{n+1}$.
- Working backwards: $r_{n-1} \mid r_1$ and $r_{n-1} \mid b$.
- From $a = bq_1 + r_1$: $r_{n-1} \mid a$.
  Therefore $r_{n-1} \mid a$ and $r_{n-1} \mid b$.
- Now let's show it's the greatest such divisor.
- Notice that we can write every number in the algorithm as a linear combination of a and b.
  - $a = bq_1 + r_1 \Rightarrow r_1 = a - bq_1 = a - (q_1)b$
  - $b = r_1 q_2 + r_2 \Rightarrow r_2 = b - r_1 q_2 = b - (a - bq_1)q_2$
    $= -q_2 \cdot a + (1 + q_1 q_2) b$
  - In general, $r_i = s \cdot a + t \cdot b$ for some integers s, t.
  - Since $r_{n-1} = s \cdot a + t \cdot b$ and any common divisor of a and b must divide all linear combinations of a and b, for all common divisors d of a and b
    $$d \mid r_{n-1} \Rightarrow d \leq r_{n-1}.$$
  - Thus $\gcd(a,b) = r_{n-1}$. □

Bézout's Identity

thm:

- Let a and b be integers with $\gcd(a,b) = d$.
- Then there exist integers x and y such that
  $ax + by = d$. ← linear diophantine equation
- Moreover, the integers of the form $az + bt$ are exactly the multiples of d.

$a = 12$, $b = 15$

x	y	$ax + by$
0	1	15
1	0	12
1	-1	-3
-1	1	3
-2	2	6
-3	3	9
⋮	⋮	⋮

proof:

- Consider,
  $$S = \{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}$$
  allows us to use WOP
- Note that $S \neq \emptyset$.
- WLOG, suppose $a \neq 0$
  - case 1: If $a > 0$, set $x = 1$ and $y = 0$
    $\Rightarrow a(1) + b(0) = a > 0 \in S$.
  - case 2: If $a < 0$, set $x = -1$ and $y = 0$
    $\Rightarrow a(-1) + b(0) = -a > 0 \in S$.
- By WOP, S has a smallest element d.
- Claim: $d = \gcd(a,b)$
- Notice that $d = as + bt$ for some integers s, t.
- Claim: $d \mid a$
- Suppose FTSOC that $d \nmid a$. Then
  $$a = dq + r \quad \text{with} \quad 0 < r < d$$
- Substituting
  $$a = (as + bt)q + r$$
  $$r = a - (asq + btq)$$
  $$= a(1 - sq) + b(-tq)$$
- Notice that $r \in S$ and $r < d = \min(S)$!
- So $d \mid a$
- Conversely, $d \mid b$.
- Thus $d \mid a$ and $d \mid b$.
- Now, WTS d is the greatest common divisor of a and b.
- Let $c \in \mathbb{N}$ be s.t. $c \mid a$ and $c \mid b$.
- Since $c \mid a$ and $c \mid b$, $c \mid ax + by$ $\forall x, y \in \mathbb{Z}$.
- In particular, $c \mid as + bt \Rightarrow c \mid d \Rightarrow c \leq d$.
- Thus, $d = \gcd(a,b)$. □

Extended Euclidean Algorithm

- given: two integers a and b with $a \geq b \geq 0$.
- goal: find integers r and s such that:

$$\gcd(a,b) = ra + sb$$

find $\gcd(234, 165)$ and integers r, s such that
$\gcd(234, 165) = r \cdot 234 + s \cdot 165$.

① forward euclidean division, recording reminder

- $234 = 165 \cdot 1 + 69 \Rightarrow 69 = 234 - 165$
- $165 = 69 \cdot 2 + 27 \Rightarrow 27 = 165 - 2 \cdot 69$
- $69 = 27 \cdot 2 + 15 \Rightarrow 15 = 69 - 2 \cdot 27$
- $27 = 15 \cdot 1 + 12 \Rightarrow 12 = 27 - 15$
- $15 = 12 \cdot 1 + 3 \Rightarrow 3 = 15 - 12$
- $12 = 3 \cdot 4 + 0$

result: $\gcd(234, 165) = 3$

② back-substitution

- $3 = 15 - 12$
$= 15 - (27 - 15)$
$= 2 \cdot 15 - 27$
$= 2(69 - 2 \cdot 27) - 27$
$= 2 \cdot 69 - 5 \cdot 27$
$= 2 \cdot 69 - 5(165 - 2 \cdot 69)$
$= 12 \cdot 69 - 5 \cdot 165$
$= 12(234 - 165) - 5 \cdot 165$
$= 12 \cdot 234 - 17 \cdot 165$
$3 = 12 \cdot 234 + (-17) 165$

Euclid's lemma

thm: If p is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

proof

- Suppose $p \nmid a$. Then $\gcd(a,p) = 1$
- WTS: $p \mid b$. $\exists k$ s.t $pk = b$.
- By Bézout's identity, $\exists x, y \in \mathbb{Z}$ s.t

$$ax + py = 1 \qquad (1)$$

- Multiplying (1) by b:

$$b(ax + py) = b$$
$$\Rightarrow (ab)x + p(by) = b \qquad (2)$$

- Since $p \mid ab$ $\exists d$ s.t $pd = ab$. (3)
- Substituting (3) into (2)

$$p(dx) + p(by) = b$$
$$\Rightarrow p(ax + by) = b$$
$$\Rightarrow p \mid d.$$

□

Fundamental Theorem of Arithmetic

- Let $n \geq 1$ be an integer.
- Then n can be factored as a product of primes in a unique way up to ordering.

proof: existence

- $P(2)$ holds since $2 = 2$.
- Suppose $P(k)$ holds $\forall k \mid 2 \leq k \leq n$.
- Now, show $k+1$ can be factored as a product of primes.
- Case 1: $n+1$ is prime.
  - Then $n+1 = n+1$.
- Case 2: $n+1$ is not prime.
  - Then $\exists a, b \in \mathbb{Z} \mid 2 \leq a \leq b \leq n$ and $n+1 = ab$.
  - Then, the strong IH tells us that a and b can be factored as a product of primes, so $n+1$ is factored as a product of primes. □

proof: uniqueness

- Suppose we have two factorizations of n:

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

where $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ and WLOG suppose $r \leq s$.

- WTS: $r = s$ and $p_1 = q_1, \ldots, q_r = q_s$.
- $p_1 \mid q_1 q_2 \cdots q_s \Rightarrow p_1 \mid q_1$ or $p_1 \mid (q_2 q_3 \cdots q_s)$
$\Rightarrow p_1 \mid q_1$ or $p_1 \mid q_2 \mid p_1 \mid (q_2 q_3 \cdots q_s)$
$\Rightarrow \ldots$
$\Rightarrow p_1 \mid q_1$ or $p_1 \mid q_2$ or $p_1 \mid q_3$ or $\ldots p_1 \mid q_s$
- After relabeling, $p_1 \mid q_1$
- Since p_1, q_1 are primes,

$$p_1 = q_1$$

$$\frac{\overset{\text{integer}}{\cancel{p_1} p_2 \cdots p_r}}{p_r} = \overset{\text{integer}}{q_1 q_2 \cdots q_2}$$
so some $q_i = p_1$

- $\cancel{p_1} p_2 \cdots p_r = \cancel{q_1} q_2 \cdots q_s$
$p_2 \cdots p_r = q_2 \cdots q_s$.
- Similarly, $p_2 = q_2$ (after relabeling), then $p_3 \cdots p_r = q_3 \cdots q_r$
$\Rightarrow p_3 = q_3$
$\vdots$
$p_r = q_r$

and $1 = q_{r+1} q_{r+2} \cdots q_s$
which is not possible unless the RHS is the empty product, so $s = r$. □

definition: binary operation
- $*$ is a binary operation on a set S if for any $a,b \in S$, $a*b \in S$.

---

definition: group
- A set G together with a binary operation $*$ forms a group $(G,*)$ if the following are satisfied.
  0. $a,b \in G$, then $a*b \in G$ — closed
  1. $a,b,c \in G$, then $(a*b)*c = a*(b*c)$ — associativity
  2. $\exists\, e \in G$ s.t $e*g = g*e = g$ $\forall g \in G$ — identity
  3. $\exists\, h \in G$ s.t $g*h = h*g = e$ $\forall g \in G$ — inverses

---

example: $G = (\mathbb{Z}_6, + \bmod 6)$

Cayley Table

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

---

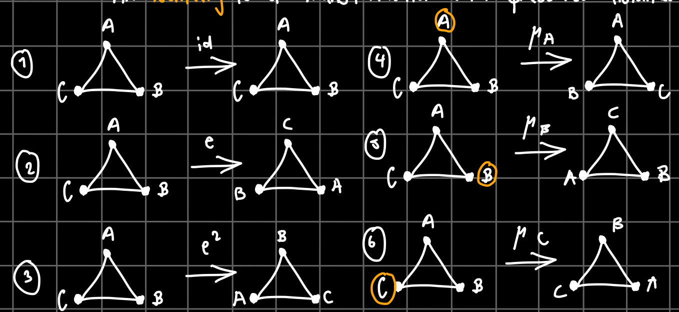
thm:
- a has an inverse mod n iff $\gcd(a,n) = 1$.

proof: ($\Leftarrow$)
- By Bézout $\exists\, x,y \in \mathbb{Z}$ s.t $ax+ny = 1$.
- Then $ax \equiv 1 \bmod n$, so x is the inverse of a mod n.

proof: ($\Rightarrow$)
- Suppose $\gcd(a,n) = 1$.
- Then $\exists\, d$ s.t $d \mid a$ and $d \mid n$.
- $d \mid ax+ny$ so $ax \not\equiv 1 \bmod n$. □

---

definition: isometry
- An **isometry** is a transformation that preserves distances.



$D_3 = \{id, e, e^2, \mu_A, \mu_B, \mu_C\}$ ▸ D_n : n = # of sides

the dihedral group of order 6, $|D_3| = 6$ ▸ D_{2n} : $2n$: # of symmetries

composition

$\circ$	id	e	e^2	μ_A	μ_B	μ_C
id	id	e	e^2	μ_A	μ_B	μ_C
e	e	e^2	id	μ_C	μ_A	μ_B
e^2	e^2	id	e	μ_B	μ_C	μ_A
μ_A	μ_A	μ_B	μ_C	id	e	e^2
μ_B	μ_B	μ_C	μ_A	e^2	id	e
μ_C	μ_C	μ_A	μ_B	e	e^2	id

smallest non-commutative group

S_n = group of permutations of n elements

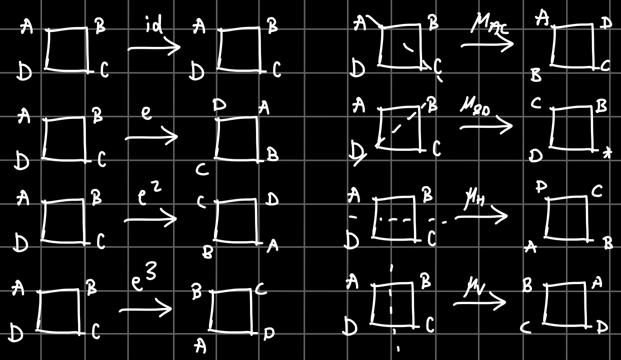
isomorphic: behaves the same
- $D_3 \cong S_3$
- $D_4 \ncong S_4$

---

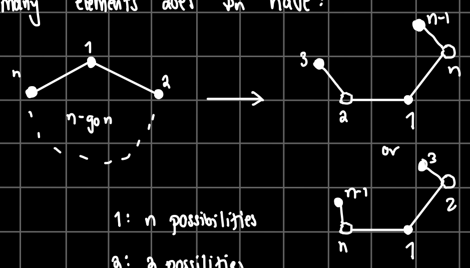
r = rotations, s = reflections

D_n = group of isometries of a regular n-gon.
- $r^n = e$
- $s^2 = e$
- $srs = r^{-1}s$

D_4



How many elements does D_n have?



1: n possibilities

2: 2 possibilities

⋮ fixed

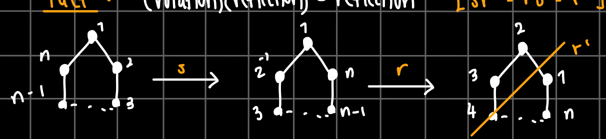
$\therefore\ |D_n| = 2n$ □

n rotations + n reflections [odd]

$\frac{n}{2}$ vertices + $\frac{n}{2}$ edges [even]

---

fact: (rotation)(reflection) = reflection $[sr^{n-1} = rs = r']$



thm: unique identity

- Let G be a group.
- It's identity is unique.

proof:

- Suppose e_1, e_2 are identities of G.
- WTS: $e_1 = e_2$.
- $\forall g \in G$, $ge = eg = g$.
- Since e_1 is an identity $e_1 e_2 = e_2$.
- Since e_2 is an identity $e_1 e_2 = e_1$.
- Thus, $e_1 = e_1 e_2 = e_2 \Rightarrow e_1 = e_2$. □

---

thm: unique inverse

- G is a group. Let $g \in G$. The inverse of g, g^{-1} is unique.

proof:

- Suppose a, b are inverses of g.
- WTS: $a = b$
- Then,

$$ag = ga = e \quad (1)$$

and, $$bg = gb = e \quad (2)$$

- Multiplying (1) by b:

$$(ag)b = eb$$

$$a(gb) = b \quad (3) \quad \text{[associativity]}$$

- Substituting (2) into (3)

$$ae = b$$

$$a = b.$$ □

---

proposition:

- Let G be a group. Suppose $a, b \in G$. Then,

$$(ab)^{-1} = b^{-1}a^{-1}$$

proof:

$(\Rightarrow)$ $$(ab)(b^{-1}a^{-1}) = a(b \cdot b^{-1})a^{-1} = (ae)a^{-1} = a \cdot a^{-1} = e$$

$(\Leftarrow)$ $$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1} \cdot a)b = b^{-1}(eb) = b^{-1} \cdot b = e.$$ □

---

proposition 3.6: every row and column are complete

- Let G be a group and $a, b \in G$.
- Then $ax = b$ and $xa = b$ have unique solutions.

proof:

- Solve $ax = b$.

$$(a^{-1} \cdot a)x = a^{-1}b$$

$$x = a^{-1}b.$$

- Solve $xa = b$.

$$x(a \cdot a^{-1}) = b \cdot a^{-1}$$

$$x = b \cdot a^{-1}$$

- $a^{-1} \cdot b \neq b \cdot a^{-1}$ □

---

proposition:

- Let G be a group and $a, b, c \in G$.
- Then,

$$ba = ca \Rightarrow b = c \quad \text{right-cancellation}$$

and

$$ab = ac \Rightarrow b = c \quad \text{left-cancellation}$$

proof:

- Suppose $ba = ca$. Then,

$$b(a \cdot a^{-1}) = c(a \cdot a^{-1})$$

$$b = c.$$

- Similarly for the other one. □

$$g^n = \underbrace{g \cdot g \cdot g \cdot g \cdots g}_{n \text{ times}}$$

$$\left.\begin{array}{l} g^0 = e \\ g^1 = g \\ g^2 = g \cdot g \\ \vdots \end{array}\right\} \forall n \in \mathbb{Z}$$

$G = (\mathbb{Z}, +)$. What is 2^{10}?

- $2^{10} = 2 + 2 + 2 + 2 + \ldots = 20$.

thm 3.8: exponent rules apply to groups

- Let $g, h \in G$.
  1) $g^m g^n = g^{m+n} \quad \forall m,n \in \mathbb{Z}$
  2) $(g^m)^n = g^{mn} \quad \forall m,n \in \mathbb{Z}$
  3) $(gh)^n = (h^{-1}g^{-1})^{-n} \quad \forall n \in \mathbb{Z}$

proof:

- if $n=0$:

$$g^m g^n = g^m e = g^m = g^{m+0}$$

- suppose $n \neq 0$:
  - If $m=0$:
    - $g^m g^n = g^n = g^{n+0}$
- If $m,n>0$:
  - $g^m g^n = \underbrace{g \cdots g}_{m} \cdot \underbrace{g \cdots g}_{n}$

$$= \underbrace{g \cdots g}_{m+n} = g^{m+n}$$

- if $m,n<0$:
  - $g^m g^n = \underbrace{g^{-1} \cdots g^{-1}}_{-m} \cdot \underbrace{g^{-1} \cdots g^{-1}}_{-n}$

$$= \underbrace{g^{-1} \cdots g^{-1}}_{-m-n} = (g^{-1})^{-m-n} = g^{m+n}$$

- if $m>0>n$ or $n>0>m$:
  - case 1: $m+n>0$
    - $\underbrace{g \cdots g}_{m+n} = g^{m+n}$
  - case 2: $m+n<0$
    - $\underbrace{g \cdots g}_{m} \underbrace{g^{-1} \cdots g^{-1}}_{-n} = \underbrace{g^{-1} \cdots g^{-1}}_{-m-n} = g^{m+n}$.
  - case 3: $m+n=0$
    - $\underbrace{g \cdots g}_{m} \underbrace{g^{-1} \cdots g^{-1}}_{-n} = e = g^0 = g^{m+n}$

definition: subgroup $\quad G \leq G \quad \& \quad \{id\} \leq G$

- $H \leq G$ if
  1) H is a subset of G
  2) H is a group with the same op operation of G.

---

thm: subgroup test

- $H \leq G$ if
  1) $e \in H \rightarrow H \neq \emptyset$
  2) $\forall a,b \in H,\ ab \in H$
  3) $\forall a \in H,\ a^{-1} \in H$.

  $\Big\}\ ab^{-1} \in H$

---

problem:

- $\mathbb{Z}_2^n = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{Z}_2\}$
- operation:

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1+b_1 \bmod 2 \dots a_n+b_n \bmod 2)$$

proof: show it's a group

① closure:

- Let $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \in \mathbb{Z}_2^n$
- NWTS: $(a_1, \dots, a_n) + (b_1, \dots, b_n) \in \mathbb{Z}_2^n$
- Let $x = (a_1+b_1 \bmod 2, \dots, a_n b_n \bmod 2)$
- Notice that $a_i + b_i \bmod 2 \in \mathbb{Z}_2 \ \forall i$
- Thus, $x \in \mathbb{Z}_2^n$.

② associativity:

- Let $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \mathbb{Z}_2$.
- $(a_1, \dots, a_n) + [(b_1, \dots, b_n) + (c_1, \dots, c_n)]$
  - $= (a_1, \dots, a_n) + (b_1+c_1, \dots, b_n c_n)$
  - $= [a_1 + (b_1+c_1), \dots, a_n + (b_n + c_n)]$
- Notice the i^{th} coordinate $a_i + (b_i + c_i) \in \mathbb{Z}_2$

  [inherited from $\mathbb{Z}_2$] $\quad = (a_i + b_i) + c_i$

  - $= [(a_1+b_1)+c_1, \dots (a_n+b_n)+c_n]$
  - $= [(a_1, \dots, a_n) + (b_1, \dots, b_n) + (c_1 + \dots + c_n)]$

③ identity:

- The identity is $(0, \dots, 0)$
- Let $(a_1, \dots, a_n) \in \mathbb{Z}_2^n$

$$(a_1, \dots, a_n) + (0, \dots, 0) = (a_1+0, \dots, a_n+0)$$
$$= (a_1, \dots, a_n).$$

  and $(0, \dots 0) + (a_1, \dots, a_n) = (a_1, \dots, a_n)$.

- Thus $(0, \dots, 0)$ is the identity.

④ inverses:

- Let $(a_1, \dots, a_n) \in \mathbb{Z}_2^n$
- $(a_1, \dots, a_n)$ is its own inverse because

$$(a_1, \dots a_n) + (a_1, \dots, a_n) = (2a_1 \bmod 2, \dots, 2a_n \bmod 2)$$
$$= (0, \dots, 0)$$

$\square$

problem: subgroups of $\mathbb{Z}_2^2$

$$\begin{tikzcd}[column sep=tiny]
 & \mathbb{Z}_2^2 \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
\{(0,0),(1,0)\} \arrow[dr, no head] & \{(0,0),(0,1)\} \arrow[d, no head] & \{(0,0),(1,1)\} \arrow[dl, no head] \\
 & \{0,0\} &
\end{tikzcd}$$

note: the only way to get subgroups of order 2 is if we have the identity and inverses

works great is elements are their own inverse

---

problem: subgroups of $\mathbb{Z}$

- $\{0\} \leq \mathbb{Z}$
- Let's say $H \leq \mathbb{Z}$.
- Suppose we know $1 \in H$.
- By closure:

$$\left.\begin{array}{l} 1+1 = 2 \in H \\ 2+1 = 3 \in H \\ \vdots \end{array}\right\} \{\mathbb{Z}^+ - 0\}$$

- By inverses: $-1 \in H$

$$\left.\begin{array}{l} -1+(-1) = -2 \in H \\ -2+(-1) = -3 \in H \\ \vdots \end{array}\right\} \{\mathbb{Z}^- - 0\}$$

- By identity: $0 \in H$

proof:

- If $n \in H \Rightarrow -n \in H$.
- Let $S = \{n \in H ; n > 0\}$
- If $H \neq \{0\}$, by WOP, S is not empty.
- Let n be the smallest element of S.
- We know $kn \in H$ $\forall k \in \mathbb{Z}$ [if $n \in H$, $n+n \in H$, $n+n+n \in H$, $\vdots$, $kn \in H$]
- $0 \in H$ because H is a group.
- If $n=1 \in H$, then $H = \mathbb{Z}$.
- Let $m \in H$.
- By the division algorithm, $\exists q, r$ s.t.

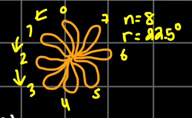
$$m = qn + r \Rightarrow r = m - qn = m + (-qn)$$

with $0 \leq r < n$.

- Notice that $qn \in H$ $\Rightarrow -qn \in H$
- Since $m \in H$, $m + (-qn) \in H$, so $r \in H$.
- By the minimality of n, $r = 0$.
- So $m \in n\mathbb{Z}$.
- So $H = n\mathbb{Z}$.

---

definition: cyclic group $C_n = \langle r \mid r^n = e \rangle$, $r = \frac{2\pi}{n}$



- A group G is cyclic if $\exists g \in G$ such that

$G = \langle g \rangle$

---

thm: infinite cyclic group

- The subgroups of $\mathbb{Z}$ are all of the form $n\mathbb{Z}$

---

thm: finite cyclic group — describe the symmetry of objects that only have rotational symmetry

- The subgroups of $\mathbb{Z}_m$ are all of the form $n\mathbb{Z}_m$.

---

given a, $\langle a \rangle$ is what you get by doing the bare minimum

thm: $\langle a \rangle$ is the smallest subgroup of G containing a.

smallest subgroup of $(G, \times)$ containing g: $\{\dots, g^{-2}, g^{-1}, id, g, g^2, \dots\}$; smallest subgroup of $(G,+)$ containing g: $\{\dots, -2g, -g, id, g, 2g, \dots\}$

proof:

- Let G be a group and $a \in G$.
  Define $\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$

1. $\langle a \rangle$ is non-empty because $a^0 = e \in \langle a \rangle$.
2. Consider $a^m \cdot a^n = a^{m+n}$. Since $m, n \in \mathbb{Z}$, so is $m+n$. Thus $\langle a \rangle$ is closed.
3. Consider $(a^n)^{-1} = a^{-n}$. Since $n \in \mathbb{Z}$, so is $-n$. Thus $\langle a \rangle$ is closed under inverse.
4. From 1-3, $\langle a \rangle$ is a subgroup of G.
5. Let H be any subgroup of G with $a \in H$. Because H is closed and has inverses, $\forall n \in \mathbb{Z}$, we have $a^n \in H$. Therefore $\langle a \rangle \leq H$.
6. Since $\langle a \rangle$ is a subgroup containing a and is contained in every subgroup that contains a, it is the smallest subgroup of G containing a.

---

thm: if $\gcd(a,n) = 1$ (relatively prime), $\mathbb{Z}_n = \langle a \rangle$ with $n > a$.

- $\phi(n) = |\{a \in \{1, 2, \dots, n\} \mid \gcd(a,n) = 1\}|$

$\mathbb{Z}_n^{\times}$

---

thm: $\mathbb{Z}_n^{\times}$ is cyclic if and only if

1) $n = 1, 2, 4$ or
2) $n = p^k$ for p an odd prime and $k \in \mathbb{N}$ or
3) $n = 2p^k$ for p an odd prime and $k \in \mathbb{N}$.

---

definition: abelian group

- When a group G is commutative, we say G is an abelian group

---

thm: every cyclic group is abelian

proof:

- Because G is cyclic, $\exists g \in G$ s.t
  $$\langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \} = G.$$
- Let $a, b \in G$.
- $\underline{\text{WTS}}$: $a \circ b = b \circ a$
- $a \in \langle g \rangle \Rightarrow a = g^A$ for some $A \in \mathbb{Z}$.
  $b \in \langle g \rangle \Rightarrow b = g^B$ for some $B \in \mathbb{Z}$.
- Then
$$\begin{aligned} a \circ b &= g^A \circ g^B && [a = g^A, b = g^B] \\ &= g^{A+B} && [\text{thm 3.8 item 1}] \quad \text{exponent rules apply to groups} \\ &= g^{B+A} && [A, B \in \mathbb{Z} \text{ and addition is comm. in } \mathbb{Z}] \\ &= g^B \circ g^A && [\text{thm 3.8 item 1}] \\ &= b \circ a. && [g^B = b, g^A = a] \end{aligned}$$

$\square$

---

thm: every subgroup H of a cyclic group G is cyclic.

proof:

- Let $H \leq G$.
- $\exists g \in G$ such $G = \langle g \rangle$ [cyclic definition]
- Let $h \in H$. Then $h = g^{k_h}$ for some $k_h \in \mathbb{Z}$. [$h \in H \subseteq G$]
- $\underline{\text{WTS}}$: $H = \langle h \rangle$
- Let $S = \{ k_h \in \mathbb{Z} \mid g^{k_h} \in H, k_h > 0 \}$ [exponents]
- $K \in S \Rightarrow g^{-k} \in H$ [$k \in S \Rightarrow g^k \in H \Rightarrow (g^k)^{-1} = g^{-k} \in H$]
- If $H = \{e\} \Rightarrow H = \langle e \rangle$.
- If $H \neq \{e\}$, $\exists h \in H$ s.t $h \neq e$.
  so $h = g^{k_h}$ for some $k_h \neq 0$.
- If $k_h < 0 \Rightarrow h^{-1} = g^{-k_h}$ and $-k_h > 0$ so $-k_h \in S$.
- If $k_h > 0 \Rightarrow k_h \in S$.
- Note, $k_h \neq 0$ since $h \neq e$.
- So $S \neq \emptyset$.
- Let n be the smallest element of S.
- Suppose $g^k \in H$.
- By the division algorithm, $\exists q, r \in \mathbb{Z}$ s.t
  $$k = nq + r \quad \text{with} \quad 0 \leq r < n$$
- We know $g^n \in H \Rightarrow g^{nq} \in H$ [closure of H]
  $\Rightarrow g^{-nq} \in H$ [inverses]
- Then
$$\begin{aligned} g^k g^{-nq} &\in H \quad [\text{closed}] \\ g^{k-nq} &\in H \\ g^r &\in H \end{aligned}$$
- Since $0 \leq r < n$ and $r < n$, $r = 0$.
- Then $k = nq$
- So $g^k = g^{nq} = (g^n)^q \in \langle g^n \rangle$.
- Thus $H \subseteq \langle g^n \rangle$.
- But $g^n \in H$, so $g^n \leq H$.
- So $H = \langle g^n \rangle$.

$\square$

---

thm: order of a power

- Let G be a finite cyclic group of order n.
- Suppose $G = \langle g \rangle$ for some $g \in G$.
- Then $$|g^a| = \frac{n}{\gcd(a, n)}$$

$|\langle g^a \rangle|$

you get a subgroup size for each divisor of n

$\mathbb{Z}_{12} = \langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
$= \langle 5 \rangle = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\}$

$$|1| = |5^5| = \frac{12}{\gcd(5, 12)} = 12$$

proof:

- We want to find the smallest $k \in \mathbb{Z}^+$ such that
$$(g^a)^k = e$$
$$g^{ak} = e$$
- $|g| = n$ because $G = \langle g \rangle$
- $G = \{e, g, g^2, \ldots, g^{n-1}\}$
- $ak \equiv 0 \bmod n$
- Suppose $\gcd(a, n) = d$. Then
$$a = da'$$
$$n = dn' \quad \text{with } \gcd(a', n') = 1.$$
- So
$$a'dk \equiv 0 \bmod n'd$$
$$a'k \equiv 0 \bmod n'$$
- Note: $n' = n / \gcd(a, n)$
- $k \equiv 0 \bmod n'$ so $n' \mid k$.
  $\Rightarrow n' \leq k$.
- $$(g^a)^{n'} = (g^a)^{n/\gcd(a,n)} = g^{an/\gcd(a,n)} = (g^n)^{a/\gcd(a,n)} = (g^n)^{a'} = e^{a'} = e.$$
- Then $k \leq n'$
- So $k = n'$.

---

thm: power rule: $(ab)^n = a^n b^n$ when G is abelian. ($n \geq 1$)

proof: We'll induct on n

- $P(1)$ holds since $(ab)^1 = ab = a^1 b^1$
- Assume $P(n)$ holds s.t $(ab)^n = a^n b^n$.
- Then
$$\begin{aligned} (ab)^{n+1} &= (ab)(ab)^n \\ &= (ab)(a^n b^n) \\ &= (a \cdot a^n)(b \cdot b^n) && [G \text{ is abelian}] \\ &= a^{n+1} b^{n+1} \end{aligned}$$

---

thm: $\forall a, g \in G$, $gag^{-1} = a$ when G is abelian. (conjugate)

proof

- Let $a, g \in G$. Then
$$\begin{aligned} gag^{-1} &= a(gg^{-1}) \\ &= ae \\ &= a. \end{aligned}$$

---

thm:

- Suppose $g \in G$ with $|g| = n$.
- Then $g^k = e \iff n \mid k$.

proof: → could also use division algorithm.

- since $|g| = n$, $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$
- so, $g^k = e \Rightarrow n \mid k$.
- If $n \mid k$, $k = an$.
- Thus, $g^k = g^{an} = (g^n)^a = e^a = e$. □

↗ the order of a finite cyclic group is the number of rotations to return to the identity denoted G_n or $\mathbb{Z}_n$

thm: order of a finite group $|G|$

- Suppose $g \in G$ where G is a finite group of order n.
- The order of g is the smallest positive integers k such that $g^k = e$.
- $G = \{\underbrace{e, g, g^2, g^3, \dots, g^n}\}$

  n+1 items, n powers } By pigeonhole, at least two are the same

$240 = 72 \cdot 3 + 24$
$72 = 3 \cdot 24 + 0$

- where $g^i = g^j$ for some $0 \le i < j \le n$.

  $\therefore e = g^{j-i}$. $\quad 0 < j-i \le n$

---

square & multiply

the method of repeated squares (modular exponentiation)

example: $3^{45} \bmod 7$

- convert 45 to binary

  $45 = 2^5 + 2^3 + 2^2 + 2^0 = 101101$
- so, we have,

  $3^{2^5+2^3+2^2+2^0} \bmod 7$

  $3^{101101_2} \bmod 7$
- notice that,

  $x^{1_2} \cdot x^{1_2} = x^{10_2}$ } squaring
  $x^{10_2} \cdot x^{10_2} = x^{100_2}$ }

  $x^{100_2} \cdot x = x^{101_2}$ → multiplication
- now, starting with 3^1

S	1→10	$3^1 \cdot 3^1 = 3^{10}$	$= 3^2 = 9 \bmod 7 = 2$
SM	10→101	$3^{10} \cdot 3^{10} = 3^{100}$	$= 3^4 = 2^2 \bmod 7 = 4$
		$3^{100} \cdot 3 = 3^{101}$	$= 3^5 = 4 \cdot 3 \bmod 7 = 5$
SM	101→1011	$3^{101} \cdot 3^{101} = 3^{1010}$	$= 3^{10} = 5^2 \bmod 7 = 4$
		$3^{1010} \cdot 3^1 = 3^{1011}$	$= 3^{11} = 4 \cdot 3 \bmod 7 = 5$
S	1011→10110	$3^{1011} \cdot 3^{1011} = 3^{10110}$	$= 3^{22} = 5^2 \bmod 7 = 4$
SM	10110→101101	$3^{10110} \cdot 3^{10110} = 3^{101100}$	$= 3^{44} = 4^2 \bmod 7 = 2$
		$3^{101100} \cdot 3 = 3^{101101}$	$= 3^{45} = 2 \cdot 3 \bmod 7 = 6$

- thus,

  $3^{45} \bmod 7 = 6$.

---

definition: permutation groups

- S_n = group of permutations on $\{1, 2, \dots, n\}$ with operation "composition".
- A permutation on $\{1, 2, \dots, n\}$ is a bijection on $\sigma : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$

example:

	1	2	3
σ_1	1	2	3
σ_2	1	3	2
σ_3	2	1	3
σ_4	2	3	1
σ_5	3	1	2
σ_6	3	2	1

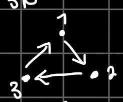
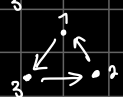
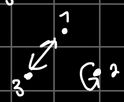
$\sigma_4 \circ \sigma_2(1) = 2$
$\sigma_4 \circ \sigma_2(2) = 1$
$\sigma_4 \circ \sigma_2(3) = 3$

$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$\sigma_4 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

---

cycle notation: factorization into disjoint cycles

- $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ =  = $(1)(2)(3) = (1)$
- $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ =  = $(1)(23) = (23)$
- $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ =  = $(12)(3) = (12)$
- $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ =  = (123)
- $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ =  = (132)
- $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ =  = $(13)(2) = (13)$

example:

- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 5 & 2 & 1 & 12 & 10 & 9 & 8 & 6 & 7 & 11 & 4 \end{pmatrix}$

$= (1\ 3\ 2\ 5\ 12\ 4)(6\ 10\ 7\ 9)(8)(11)$
$= (1\ 3\ 2\ 5\ 12\ 4)(6\ 10\ 7\ 9)$ //

---

thm: cycle order

- cycles with no numbers in common (disjoint) commute with each other.

  because each number is only affected by 1 cycle so the order of the cycles doesn't matter

definition: transpositions
- 2-cycles are called transpositions

lemma: every cycle is a product of transpositions.

anchor-at-first

$$(a_1\ a_2 \dots a_n) = (a_1\ a_n)(a_1\ a_{n-1})(a_1\ a_{n-2})\dots(a_1\ a_2)$$

OR

$$(a_1\ a_2)(a_2\ a_3)(a_3\ a_4)\dots(a_{n-1}, a_n)$$

consecutive pairs

proof:
- Let's evaluate

  $\sigma = (a_1\ a_n)(a_1\ a_{n-1})\dots(a_1\ a_2)$
- Plug in a_k $(a_1\ a_n)(a_1\ a_{n-1})\dots(a_1\ a_{k+2})(a_1\ a_{k+1})(a_1\ a_k)\dots(a_1\ a_2)$
- If $k \notin \{1, 2, \dots, n\}$

  $\Rightarrow \sigma(a_k) = a_k$.
- Suppose $k = n$. Then,

  $\sigma(a_n) = a_1$
- Suppose $k \leq n-1$.

  $(a_1\ a_{k-1})(a_1\ a_{k-2})\dots(a_1\ a_2)$ all leave a_k fixed

  $(a_1\ a_k)(a_k) = a_1$

  $(a_1\ a_{k+1})(a_1) = a_{k+1}$

  $(a_1\ a_{k+2})(a_1\ a_{k+3})\dots(a_1\ a_n)$ all leave a_{k+1} fixed

  $\Rightarrow \sigma(a_k) = a_{k+1}$
- Thus $\sigma = (a_1\ a_2 \dots a_n)$ □

---

definition: permutation parity
- A permutation $\sigma \in S_n$ is even if it can be written as a product of an even number of transpositions.
- Otherwise, σ is odd.

---

inverse: $(\underbrace{a_1 \dots a_n}_{\text{reverse}})^{-1} = (a_1\ a_n\ a_{n-1} \dots a_2)$

corollary:
- Suppose $\tau_1, \tau_m, \theta_1, \theta_2, \dots, \theta_k \in S_n$ are transpositions such that

  $\tau_1\tau_2\dots\tau_m = \theta_1\theta_2\dots\theta_k$.
- Then $m-k$ is even.

proof:
- $\underbrace{\tau_1\tau_2\dots\tau_m\theta_k\theta_{k-1}\dots\theta_1}_{m+k \text{ transpositions}} = \theta_1\theta_2\dots\theta_k\theta_k\theta_{k-1}\dots\theta_1 = (1)$
- By the theorem, $m+k$ is even.
- So $m-k = (m+k) - 2k$ is also even.

---

examples:
1. $(1\ 2\ 3) = (1\ 2)(1\ 3)$ even
2. $(1\ 2)$ odd
3. $(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$ odd

thm:
- Let $\sigma, \rho \in S_n$ and are disjoint cycles.
- Then $\sigma\rho = \rho\sigma$.

proof:
- Let $\sigma = (s_1\ s_2 \dots s_k)$

  $\rho = (r_1\ r_2 \dots r_m)$
- Then,

$$\sigma\rho(x) = \begin{cases} x & \text{if } x \notin \{s_1, \dots, s_k, r_1, \dots r_m\} \\ r_{i+1} & \text{if } x \in \{r_1, \dots, r_m\} \\ r_1 & \text{if } x = r_m \\ s_{i+1} & \text{if } x \in \{s_1, \dots, s_k\} \\ s_1 & \text{if } x = s_k \end{cases}$$

$$= \rho\sigma(x)$$

---

thm.
- Suppose $\tau_1, \tau_2, \dots, \tau_m$ are transpositions such that

  $\tau_1, \tau_2, \dots, \tau_m = (1)$, identity

  then m is even.

pre-proof:
- For any transposition, we have 4 cases.
  1. $\tau_{m-1}\tau_m = (ab)(ab) = (1)$
  2. $\tau_{m-1}\tau_m = (bc)(ab) = (ac)(bc)$
  3. $\tau_{m-1}\tau_m = (ac)(ab) = (ab)(bc)$
  4. $\tau_{m-1}\tau_m = (cd)(ab) = (ab)(cd)$

proof:
- Let $\tau_1\tau_2 = \tau_{m-1}\tau_m$
- If $m = 1$ ↯ $\tau_1 \neq (1)$
- If $m = 2$ $\tau_1\tau_2 = (1)$, 2 is even ✓
- I.H. If $k \leq m-1$, then $\tau_1\tau_2\dots\tau_k = (1) \Rightarrow 2 \mid k$.
- $\tau_1\tau\dots\tau_{m-1}$

  $(a\ x)$
- We can do the same process to get either 2 transpositions that cancel, then either the I.H concludes the proof or we can keep pushing until it cancels.
- For "a" not to cancel, it would reach the first transposition and not be anywhere else

  $\sigma = (a\ x)\underbrace{\tau_2'\ \tau_3' \dots \tau_m'}_{\text{no } a\text{'s}}$

  so, $\sigma(a) = x$

  $\sigma = (1)$

  so $\sigma(a) = a$ ↯

thm:

- The set of even transpositions
  $A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\} \leq S_n$.

proof:

① $A_n \subseteq S_n$

② $\sigma \in A_n \Rightarrow \sigma \in S_n$. ✓
 (1) is even so $(1) \in A_n$ ✓

③ Suppose $\sigma_1, \sigma_2 \in A_n$. Then $\exists\ \tau_1, \tau_2, \dots, \tau_{2k} \in S_n$
 $\theta_1, \theta_2, \dots, \theta_{2m} \in S_n$
 transpositions such that
 $\sigma_1 = \tau_1\tau_2 \dots \tau_{2k}$
 $\theta_2 = \theta_1\theta_2 \dots \theta_{2m}$

- so $\theta_1\theta_2 = \tau_1\tau_2 \dots \tau_{2k}\ \theta_1\theta_2 \dots \theta_{2m}$
- The $\sigma_1\sigma_2$ is the product of $2k+2m$ transpositions, which is even.
- So $\sigma_1\sigma_2 \in A_n$.

④ Suppose $\sigma_1 = \tau_1\tau_2 \dots \tau_{2k} \in A_n$
 The $\sigma_1^{-1} = \tau_{2k}, \tau_{2k-1} \dots \tau_1 \in A_n$.

- Thus, $A_n \leq S_n$. □

---

thm: $|A_n| = \frac{n!}{2}\ \forall n \geq 2$. ($n!$ → all permutations)

proof:

- Let $\tau = (1\ 2) \in S_n$
- Let $\sigma \in A_n$.
 $f: A_n \to S_n$
 $f(\sigma) = \tau\sigma$
- claim: f is 1-1.
 proof: Suppose $f(\sigma_1) = f(\sigma_2)$
 then $\tau\sigma_1 = \tau\sigma_2$
 so $\sigma_1 = \sigma_2$. [left-cancellation]
- So $|A_n| = |\text{Im} f|$
- If $\mu \in \text{Im} f$, then
 $\mu = \tau\sigma$ for some $\sigma \in A_n$, so μ is odd.
 σ is even so its a product of an even number of $2k$ transpositions. So μ is the product of $2k+1$ of them.
- Let B_n be the set of all odd permutations.
- So $|A_n| = |\text{Im} f| \leq |B_n|$
- $g: B_n \to S_n$
 $g(\mu) = \tau\mu$
 g is 1-1.
- So $|B_n| = |\text{Im}\, g| \leq |A_n|$
- So $|A_n| = |B_n|$
- $g(\mu)$ is even.
- $|A_n| + |B_n| = |S_n| = n!$
 $2|A_n| \Rightarrow |A_n| = \frac{n!}{2}$

definition: dihedral groups as permutations

- The dihedral group is the group of isometries of a regular n-gon.

example: D_4

- $D_4 = \{(1), (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2),$
 $(1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3), (2\ 4)\}$
- The cayley table is then just cycle products.

example: D_5

- $D_5 = \{(1), \underset{}{\overset{r}{(1\ 2\ 3\ 4\ 5)}}, \overset{r^2}{(1\ 3\ 5\ 2\ 4)}, \overset{r^3}{(1\ 4\ 2\ 5\ 3)},$
 $\overset{r^4}{(1\ 5\ 4\ 3\ 2)}, \overset{s\ (\text{fix } 1)}{(2\ 5)(3\ 4)}, \overset{sr\ (\text{fix } 5)}{(1\ 4)(2\ 3)}, \overset{sr^2\ \text{fix}(4)}{(1\ 2)(3\ 5)},$
 $\overset{sr^3\ (\text{fix } 3)}{(1\ 5)(2\ 4)}, \overset{sr^4\ (\text{fix } 2)}{(1\ 3)(2\ 4)}\}$

---

definition: alternative dihedral group definition.

- $D_n = \left\{ r^a s^b \;\middle|\; \begin{matrix} 0 \leq a \leq n-1 \\ 0 \leq b \leq 1 \end{matrix},\ r^n = e,\ s^2 = e,\ rs = sr^{n-1} \right\}$
 $r^k \neq e\ \forall k,\ 0 \leq k \leq n-1$
 $s \neq e$

- $D_n = \{e, r, r^2, \dots, r^{n-1},$
 $s, rs, r^2s, \dots, r^{n-1}s\}$
 ↓
 all unique.

 if $r^i = r^j \Rightarrow r^i r^{-j} = 1$
 $r^{i-j} = 1$
 $\Rightarrow |r| \mid i-j$
 $|r| = n$.
 $n \mid i-j$ so $i-j \equiv 0 \bmod n$
 $\Rightarrow i = j$.

if $|s| = 2$ $(s^2 = e)$
then, $(sgs)^n = sg^n s$
↓
$sgs \cdot sgs \dots sgs\ sgs$
$s \cdot \underbrace{g \dots g}_{n \text{ times}} \cdot s$

---

thm: $r^a s = sr^{n-a}$

---

definition: coset

- Let $H \leq G$
- Let $g \in G$.
- The left coset of H generated by g is
  $$gH = \{gh \mid h \in H\}$$
- The right coset of H generated by g is
  $$Hg = \{hg \mid h \in H\}$$

example:

- $G = \mathbb{Z}_6$
- $H = \{0, 3\}$
  - $0 + H = \{0, 3\}$
  - $1 + H = \{1, 4\}$
  - $2 + H = \{2, 5\}$
  - $3 + H = \{3, 0\}$
  - $4 + H = \{4, 1\}$
  - $5 + H = \{5, 2\}$

---

lemma: coset order

- Suppose G is a group and $H \leq G$.
- Let $g \in G$. Then,
  $$|H| = |gH|$$

proof:

- Let $f: H \to gH$
  $f(h) = gh$.
- Let's prove it's a bijection.
- onto: Let $x \in gh \Rightarrow \exists h \in H$ s.t. $x = gh$. Then $f(h) = x$ so f is onto.
- 1-1: Suppose $f(h_1) = f(h_2) \Rightarrow gh_1 = gh_2 \Rightarrow h_1 = h_2$ by left-cancellation. So f is 1-1.
- Since f is a bijection $|H| = |gH|$

---

lemma: cosets are disjoint

→ that means if $c \in c(H)$, any coset with the element c is just $c(H)$.

- Let $g_1, g_2 \in G$, $H \leq G$.
- If $g_1H \cap g_2H \neq \emptyset$ then
  $$g_1H = g_2H$$

proof:

- Suppose $g_1H \cap g_2H \neq \emptyset$.
- Then $\exists x \in g_1H \cap g_2H$. $\Rightarrow x = g_1h_1$ for some $h_1 \in H$
  $x = g_2h_2$ for some $h_2 \in H$
- Then, $g_1h_1 = g_2h_2$.
- Let $a \in g_1H$. WTS $a \in g_2H$.
- $a = g_1h$ for some $h \in H$.
- Recall $g_1h_1 = g_2h_2 \Rightarrow g_1 = g_2h_2h^{-1}$
- So $a = g_2h_2h^{-1}h = g_2(h_2h^{-1}h) \in g_2H$.
- So $a \in g_2H$
  $\Rightarrow g_1H \subseteq g_2H$.
- Now suppose $b \in g_2H$. WTS $b \in g_1H$.
- $b = g_2h' = (g_1h_1h_2^{-1})h' = g(h_1h_2^{-1}h')$
- So $b \in g_1H$
  $\Rightarrow g_2H \subseteq g_1H$.
- Then $g_1H = g_2H$

---

lemma. cosets partition G

- Let G be a group. $H \leq G$.
- The left cosets of H partition G.

proof:

- For any $g \in G$, $g \in gH$ because $e \in H$
- Then $G \subseteq \bigcup_{g \in G} gH$
- Take $x \in gH \Rightarrow x = gh$ for some $h \in H$ but $h \in G$ so $gh \in G$ so $gH \subseteq G$.
- Therefore $\bigcup_{g \in G} gH \subseteq G$.
- So, $G = \bigcup_{g \in H} gh$.
- By the previous lemma, any two distinct cosets are disjoint so the cosets partition G.

---

thm: Lagrange's theorem

- Let $|G| < \infty$ be a group.
- Let $H \leq G$. Then $\rightarrow [G:H] = \frac{|G|}{|H|}$

$|H| \mid |G|$

proof:

- $G = \bigcup_{g \in G} gH$
- Each coset has the same size as $|H|$.
- So, $|G| = m|H|$ where m is the number of cosets.
- Therefore $|H| \mid |G|$

---

definition: number of cosets

- $[G:H] = $ # of cosets of H in G. $= \frac{|G|}{|H|}$

index of H in G

---

example:

- $G = \mathbb{Z}$
- $H = 6\mathbb{Z} = \{6k \mid k \in \mathbb{Z}\}$
- $[G:H] = 6$

- $H = \{6k \mid k \in \mathbb{Z}\}$
- $1+H = \{6k+1 \mid k \in \mathbb{Z}\}$
- $2+H = \{6k+2 \mid k \in \mathbb{Z}\}$
- $3+H = \{6k+3 \mid k \in \mathbb{Z}\}$
- $4+H = \{6k+4 \mid k \in \mathbb{Z}\}$
- $5+H = \{6k+5 \mid k \in \mathbb{Z}\}$

---

thm: groups with prime order are cyclic

- Let G be a group of size p where p is prime.
- Then G is cyclic.

proof:

- Since $p \geq 2$. We can take $g \in G / \{e\}$.
- Then $H = \langle g \rangle$ is a subgroup of G.
- Since $g \neq e$, $|H| > 1$ $(e, g \in H)$
- By Lagrange, $|H| \mid |G| = p$.
- Since $|H| \neq 1$, $|H| = p$.
- So $H = G$.
- So $G = \langle g \rangle$.

---

example:

- $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- $H = \{(0,0,0), (1,1,1)\}$
- what are the cosets of H in G?

$G = \{(0,0,0), (1,1,1), (1,0,0), (1,0,1),$
$(1,1,0), (0,0,1), (0,1,0), (0,1,1)\}$

$(0,0,0) + H = \{(0,0,0), (1,1,1)\} = (1,1,1) + H$
$(1,0,0) + H = \{(1,0,0), (0,1,1)\} = (0,1,1) + H$
$(1,0,1) + H = \{(1,0,1), (0,1,0)\} = (0,1,0) + H$
$(1,1,0) + H = \{(1,1,0), (0,0,1)\} = (0,0,1) + H$

---

example:

- Suppose $G = \mathbb{Z}_{11}^{\times}$
- $|\mathbb{Z}_{11}^{\times}| = 10$
- $2 \in \mathbb{Z}_{11}^{\times}$
- $\langle 2 \rangle = \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\}$

$|2| = 10$
- $\langle 3 \rangle = \{1, 3, 9, 5, 4\}$

$|3| = 5$

---

thm. the order of an element divides the order of the group.

- Suppose $|G| = n$
- Let $a \in G$ with $|a| = k$

$\Rightarrow a^k = e$
- By Lagrange, $k \mid n$

$\Rightarrow a^n = (a^k)^{\frac{n}{k}} = e^{\frac{n}{k}} = e$
- So $a^n = e$ in G.

---

thm: Fermat's Little Theorem

- Let p be a prime and $a \in \mathbb{Z}$ such that $p \nmid a$. Then,

$a^{p-1} \equiv 1 \mod p$

proof:

since $p \nmid a$, there's a remainder

- Let $G = \mathbb{Z}_p^{\times} = \{1, 2, \ldots, p-1\}$
- $p \nmid a \Rightarrow a \equiv i \mod p$ for some $i \in \mathbb{Z}_p^{\times}$
- $|\mathbb{Z}_p^{\times}| = p-1$.
- Let $k = |a| \Rightarrow a^k = e = 1$
- By Lagrange, the order of an element a must divide the order of the group. Which is $p-1$.

$k \mid p-1$

$\Rightarrow p-1 = k \cdot m$ for some $m \in \mathbb{Z}$
- Then, $a^{p-1} = a^{km} = (a^k)^m \equiv 1^m \equiv 1 \mod p$ □

thm: Euler's Totient Theorem

- Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that $\gcd(a,n) = 1$ (i.e, a and n are coprime. Then:

$$a^{\phi(n)} \equiv 1 \mod n$$

where $\phi(n) = |\{1 \leq k \leq n \mid k \in \mathbb{Z}, \gcd(k,n) = 1\}|$ (i.e, number of elements coprime to n).

proof:

- Let $G = \mathbb{Z}_n^{\times}$
- Then $|\mathbb{Z}_n^{\times}| = \phi(n)$
- Since $\gcd(a,n) = 1$, $a \in G$.
- Let $k = |a|$. $\Rightarrow a^k = 1$
- By lagrange, $k \mid \phi(n) \Rightarrow \phi n = k \cdot m$ for some $m \in \mathbb{Z}$.
  Then, $a^{\phi(n)} = a^{km} = (a^k)^m \equiv 1^m \equiv 1 \pmod n$

---

thm:

- Let G be a finite group.
- Suppose H and K are subgroups of G satisfying

$$K \subseteq H \subseteq G$$

- Then:

$$[G:K] = [G:H] \cdot [H:K]$$

proof:

- $[G:H] \cdot [H:K] = \frac{|G|}{\cancel{|H|}} \cdot \frac{\cancel{|H|}}{|K|} = \frac{|G|}{|K|} = [G:K]$

---

inverse of lagrange's theorem

can we find a subgroup for every divisor of n.

thm: A_4 has no subgroups of order 6.

proof:

- $A_4 = \{(1), (123), (132), (134), (143), (234), (243), (124), (142), (12)(34), (13)(24), (14)(23)\}$
- $|A_4| = 12$
- Suppose there is a subgroup H of order 6.
- By Lagrange, $[A_4 : H] = \frac{|A_4|}{|H|} = \frac{12}{6} = 2$
- There are 2 cosets of H in A_4
- Since H is one of the cosets, the left = the right: $gH = Hg$ ($gHg^{-1} = H$)
- H has at least 2 3-cycles. either $\mathbb{Z}_6$ or S_3
- WLOG, suppose $(123) \in H$
- Then $(123)^{-1} = (132)$ must also be in H.
- Since $ghg^{-1} \in H$ for all $g \in A_4$ and all $h \in H$.

subgroups of order 2 are normal and the closure of conjugates always holds.

$$(124)(123)(124)^{-1} = (124)(123)(142) = (243)$$

$$(243)(123)(243)^{-1} = (243)(123)(234) = (142)$$

- Thus, $H = \{(1), (123), (132), (243), (234), (124), (142)\}$
- Thus, H must have at 7 elements.
- Therefore, H cannot have order 6.

---

thm:

- Let τ, μ be cycles in S_n.
- τ and μ have the same length if and only if there exists $\sigma \in S_n$ such that

$$\mu = \sigma \tau \sigma^{-1}$$

proof:

($\Rightarrow$) Suppose τ and μ have the same length. So

$\tau^k = e$ $\quad \tau = (a_1\ a_2\ \dots\ a_k)$

$\mu^k = e$ $\quad \mu = (b_1\ b_2\ \dots\ b_k)$

for some $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k \in \{1, 2, \dots, n\}$.

- Let $\sigma \in S_n$ satisfy

$$\sigma(a_1) = b_1$$
$$\sigma(a_2) = b_2$$
$$\vdots$$
$$\sigma(a_n) = b_n$$

if $x \notin \{a_1, a_2, \dots, a_n\}$ choose $\sigma(x)$ to be something left

- $\sigma\tau\sigma^{-1}(b_i) = \sigma\tau(a_i) = \sigma(a_{i+1 \bmod k}) = b_{i+1 \bmod k}$
- Suppose $x \notin \{b_1, \dots, b_k\}$
- $\sigma\tau\sigma^{-1}(x) = \sigma\tau(\sigma^{-1}(x)) = \sigma(\sigma^{-1}(x)) = x$
- So $\sigma\tau\sigma^{-1}$ sends $b_1 \to b_2$, $\vdots$, $b_k \to b_1$, $x \to x$
- This is exactly μ.

($\Leftarrow$) Suppose τ, μ are cycles and $\mu = \sigma\tau\sigma^{-1}$

- WTS: τ and μ have the same length.
- Let $\tau = (a_1\ a_2\ \dots\ a_k)$
- Let $\sigma \in S_n$
- Let's show $\sigma\tau\sigma^{-1}$ is a cycle of length k.
- If $\sigma^{-1}(x) \notin \{a_1 \dots a_k\}$, then

$$\sigma\tau\sigma^{-1}(x) = \sigma\tau(\sigma^{-1}(x)) = \sigma(\sigma^{-1}(x)) = x$$

- If $\sigma^{-1}(x) = a_i$ for some i, then

$$\sigma\tau\sigma^{-1}(x) = \sigma\tau(a_i) = \sigma(a_{i+1})$$

- But $\sigma^{-1}(x) = a_i \Rightarrow x = \sigma(a_i)$
- Let $b_1 = \sigma(a_1)$

$$b_2 = \sigma(a_2)$$
$$\vdots$$
$$b_k = \sigma(a_k)$$

- Then $\sigma\tau\sigma(b_i) = b_{i+1}$ and $\sigma\tau\sigma(x) = x$ when $x \notin \{b_1 \dots b_k\}$

So

$$\sigma\tau\sigma^{-1} = (b_1\ b_2\ \dots\ b_k)$$

thm:

- Suppose $\mu \in S_n$ has cycle type $(n_1, n_2 \ldots n_k)$ where $n_1 + n_2 + \ldots + n_k = n$.
- Then for any $\sigma \in S_n$, $\sigma \mu \sigma^{-1}$ has the same cycle type as μ.

proof:

- Let $\mu = c_1 c_2 \cdots c_k$ where $c_1, c_2, \ldots, c_k$ are disjoint cycles of lengths $n_1, n_2, \ldots, n_k$, respectively.
- $\sigma \mu \sigma^{-1} = \sigma (c_1 c_2 \cdots c_k) \sigma^{-1}$
  $= (\sigma c_1 \sigma^{-1})(\sigma c_2 \sigma^{-1}) \ldots (\sigma c_k \sigma^{-1})$
  $= d_1 d_2 \ldots d_k$

  where d_i is a cycle of length n_i.
- so $\sigma \mu \sigma^{-1}$ has the same cycle type a μ.

---

definition: isomorphism

- $(G, *)$ and $(H, \circ)$ are isomorphic if there exists a function $\phi : G \to H$ where ϕ is a bijection and operation preserving.

  homomorphism

  $$\phi(g_1 * g_2) = \phi(g_1) \circ \phi(g_2)$$
- ϕ is an isomorphic and $G \cong H$.

---

claim: $\mathbb{Z}_4 \cong \mathbb{Z}_5^\times$

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$

proof:

- Let $\phi : \mathbb{Z}_5^\times \to \mathbb{Z}_4$

  $\phi(1) = 0$

  $\phi(2) = 1$

  $\phi(3) = 3$

  $\phi(4) = 2$.

$\mathrm{ord}_5 2 = 4$

$2^0 = 1 \mod 5$

$2^1 = 2 \mod 5$

$2^2 = 4 \mod 5$

$2^3 = 3 \mod 5$

- ϕ is clearly a bijection

x	y	xy	$\phi(xy)$	$\phi(x)$	$\phi(y)$	$\phi(x+y)$
1	1	1	0	0	0	0
1	2	2	1	0	1	1
1	3	3	3	0	3	3
1	4	4	2	0	2	2
2	2	4	2	1	1	2
2	3	1	0	1	3	0
2	4	3	3	1	2	3
3	3	4	2	3		2
3	4	2	1	3		1
4	4	1	0	2		0

thm:

- Suppose $\phi : G \to H$ is an isomorphism.
- Let e_G be the identity of G and e_H be the identity of H.
- Then $\phi(e_G) = e_H$.

proof:

- Let $\phi(e_G) = x$
- $\phi(e_G \cdot e_G) = \phi(e_G) = x$
  $\|$
  $\phi(e_G) \cdot \phi(e_G) = x^2$
- so $x^2 = x$, so
  $x \cdot x = x \cdot e_H$

  so $x = e_H$ (left cancellation)

---

thm: finite cyclic groups are isomorphic to $\mathbb{Z}_n$

- Suppose G is a cyclic group of order n. Then,
  $G \cong \mathbb{Z}_n$.

proof:

- G is cyclic so $\exists\, g \in G$ such that
  $\langle g \rangle = G$.
- Since G has order n, then
  $G = \{g^0, g^1, \ldots, g^{n-1}\}$
- Let $\phi : \mathbb{Z}_n \to G$
  $\phi(m) = g^m$

  $\phi(0) = e$

  $\phi(1) = g$

  $\phi(n-1) = g^{n-1}$
- ϕ is clearly a bijection
- Let $m_1, m_2 \in \mathbb{Z}_n$
- WTS: $\phi(m_1 + m_2) = \phi(m_1) \cdot \phi(m_2)$
- $\phi(m_1 + m_2) = g^{m_1 + m_2}$
  $= g^{m_1} g^{m_2}$
  $= \phi(m_1) \cdot \phi(m_2)$

---

thm:

- If G is an infinite cyclic group, then
  $G \cong \mathbb{Z}$.

proof:

- There exists $g \in G$ such that $G = \langle g \rangle$
- Suppose $g^a = g^b$ with $a \neq b$ for some a and b.
- Then $g^{a-b} = e$.
- So $|g| \mid a-b$ so G is finite !
- Therefore $\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, e, g^1, g^2, \ldots\}$
- Let $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = g^n$.
- The function is 1-1.
- ϕ is onto because if $x \in \langle g \rangle$ then $x = g^m$ for some $m \in \mathbb{Z}$ so $\phi(m) = g^m = x$.
- Therefore ϕ is a bijection.
- Let $m, n \in \mathbb{Z}$. $\phi(m+n) = g^{m+n} = g^m \cdot g^n = \phi(m)\,\phi(n)$.
- So ϕ is a bijective homomorphism. ϕ is an isomorphism. $\square$

definition: homomorphism.

- Let G and H be groups

$$\phi: G \to H$$

is a homomorphism if $\forall g_1, g_2 \in G$

$$\phi(g_1 g_2) = \phi(g_1)\,\phi(g_2)$$

preserves the group operation

---

thm:

- Let G, H be groups. Let $\phi: G \to H$ be an isomorphism.
- Then the following are true.
  1. $\phi^{-1}: H \to G$ is an isomorphism
  2. $|G| = |H|$
  3. If G is abelian, H is abelian
  4. If G is cyclic, H is cyclic.
  5. If G has a subgroup of order n, H has a subgroup of order n.

proof: 1

- Since ϕ is a bijection, ϕ^{-1} is a bijection.

Let's prove it.

ϕ^{-1} is 1-1: $\phi^{-1}(h_1) = \phi^{-1}(h_2)$

exists because ϕ is onto and $\exists! g_1 = \phi^{-1}(h_1)$ because ϕ is 1-1.

$$\phi(\phi^{-1}(h_1)) = \phi(\phi^{-1}(h_2))$$

$$h_1 = h_2 \quad ✓$$

ϕ^{-1} is onto: Let $g \in G$. WTS $\exists h \in H$ s.t $g = \phi^{-1}(h)$

Let $h = \phi(g)$. Then $\phi^{-1}(h) = \phi^{-1}(\phi(g)) = g$ ✓

ϕ^{-1} is homomorphic: Let $h_1, h_2 \in H$.

$$\phi^{-1}(h_1 h_2) = \phi^{-1}(h_1)\,\phi^{-1}(h_2)$$

$$\phi(\phi^{-1}(h_1 h_2)) = h_1 h_2$$

$$\phi(\phi^{-1}(h_1)\,\phi^{-1}(h_2)) = \phi(\phi^{-1}(h_1)) \cdot \phi(\phi^{-1}(h_2))$$

$$= h_1 h_2$$

so $\phi(\phi^{-1}(h_1 h_2)) = \phi(\phi^{-1}(h_1)\,\phi^{-1}(h_2))$ but ϕ is 1-1

$$\phi^{-1}(h_1 h_2) = \phi^{-1}(h_1)\,\phi^{-1}(h_2)$$

proof: 2

- ϕ is a bijection, therefore $|G| = |H|$

proof: 3

- Let $h_1, h_2 \in H$.
- Let $g_1, g_2 \in G$ s.t $\phi(g_1) = h_1$; $\phi(g_2) = h_2$
- $\phi(g_1 g_2) = \phi(g_1)\,\phi(g_2) = h_1 h_2$

  $\phi(g_2 g_1) = \phi(g_2)\,\phi(g_1) = h_2 h_1$
- So $h_1 h_2 = h_2 h_1$ $\therefore$ H is abelian.

proof: 4

- WTS $\exists h \in H$ such that $H = \langle h \rangle$
- Let $g \in G$ such that $G = \langle g \rangle$
- Let's prove $H = \langle h \rangle$. By definition, we know $\langle h \rangle \leq H$.
- Let $\phi(g) = h$. Let $x \in H \Rightarrow \exists y \in G$ s.t $\phi(y) = x$
- Since $y \in G$, $y = g^k$ for some integer k.
- Suppose $k \geq 0$.
- When $k = 0$, $y = e_G$ so $x = e_H \in \langle h \rangle$.

  $\phi(g^0) = h^0$
- When $k = 1$: $\phi(g^1) = h$ by definition.
- When $k = 2$: $\phi(g^2) = \phi(g \cdot g) = \phi(g) \cdot \phi(g) = h \cdot h = h^2$.
- Suppose $\phi(g^m) = h^m$

$$\phi(g^{m+1}) = \phi(g^m \cdot g) = \phi(g^m) \cdot \phi(g)$$

$$= h^m \cdot h = h^{m+1}$$

- Now suppose $k < 0$. WTS $\phi(g^{-1}) = h^{-1}$.
- $\phi(g)\,\phi(g^{-1}) = \phi(g g^{-1}) = \phi(e_G) = e_H$.
- so $\phi(g^{-1}) = (\phi(g))^{-1} = h^{-1}$
- Suppose $\phi(g^{-m}) = h^{-m}$

$$\phi(g^{-(m+1)}) = \phi(g^{-m} \cdot g^{-1})$$

$$= \phi(g^{-m}) \cdot \phi(g^{-1})$$

$$= h^{-m}\, h^{-1} = h^{-(m+1)} \quad ✓$$

- $x = \phi(y) = \phi(g^k) = h^k \in \langle h \rangle$

  so $H = \langle h \rangle$ so H is cyclic.

proof: 5

- Let K be a subgroup of G of order n,

  so $K = \{k_1, k_2, \dots, k_n\}$.
- $\phi(K) = \{\phi(k_1), \phi(k_2), \dots, \phi(k_n)\}$.
- Since ϕ is 1-1, $\phi(k_1), \phi(k_2) \dots \phi(k_n)$ are all distinct
- so $|\phi(K)| = n$.
- $\phi(K) \subseteq H$ because $\phi(k_i) \in H$. WTS: $\phi(K) \leq H$
- Since $K \leq G$, $e_G \in K$. $\phi(e_G) = e_H$. so $e_H \in \phi(K)$.
- Let $\phi(k_i), \phi(k_j) \in \phi(K)$

  $\phi(k_i)\,\phi(k_j) = \phi(k_i k_j)$

  $k_i k_j \in K$ because K is a group.

  so $\phi(k_i k_j) \in \phi(K)$
- Let $\phi(k_i) \in \phi(K)$. WTS $\phi(k_i)^{-1} \in \phi(K)$.
- K is a group so $k_i^{-1} \in K$. So $\phi(k_i^{-1}) \in \phi(K)$

  $\Rightarrow \phi(k_i)^{-1} \in \phi(K)$.

---

thm:

- two groups are related if they are isomorphic.
- this relation is an equivalence relation.

proof:

1. reflexive:
   - Let G be a group WTS $G \cong G$
   - Let $\phi(g) = g$ $\forall g \in G$.
   - This is an isomorphism. $\phi(g_1 g_2) = g_1 g_2$ & $\phi(g_1)\phi(g_2) = g_1 g_2$.
2. symmetric:
   - Let G and H be groups s.t $G \cong H$. WTS $H \cong G$.
   - Let $\phi: G \to H$ be an isomorphism.

     Then $\phi^{-1}: H \to G$ is an isomorphism. So $H \cong G$.
3. transitive:
   - Let G, H, K be groups s.t $G \cong H$ and $H \cong K$. WTS $G \cong K$.
   - $\exists\, \phi$ $G \to H$ and $\exists\, \mu: H \to K$.
   - $\mu \circ \phi: G \to K$ is a bijection.
   - Let $g_1, g_2 \in G$. WTS $\mu \circ \phi(g_1 g_2) = (\mu \circ \phi(g_1))(\mu \circ \phi(g_2))$

$$\begin{aligned} \mu \circ \phi(g_1 g_2) &= \mu(\phi(g_1 g_2)) \\ &= \mu(\phi(g_1)\phi(g_2)) \\ &= \mu(\phi(g_1))\,\mu(\phi(g_2)) \\ &= \mu \circ \phi(g_1) \cdot \mu \circ \phi(g_2) \end{aligned}$$

   - So $\mu \circ \phi$ is an isomorphism and $G \cong K$.

---

thm: Cayley's Theorem

A finite group of order n is isomorphic to a subgroup of S_n.

- Every finite group is isomorphic to a permutation group.

  $G \cong S_n$ for some n.
- Note: A finite group G is a finite permutation group if there exists n such that $G \le S_n$.

proof:

- Let G be a group.
- For $g \in G$, let $\lambda_g: G \to G$ where $\lambda_g(g') = g \cdot g'$ (bijection) (computes Cayley table rows)
- Notice that $\lambda_{g_1} \circ \lambda_{g_2} = \lambda_{g_1 g_2}$

  $\lambda_{g_1} \circ \lambda_{g_2}(g) = \lambda_{g_1}(\lambda_{g_2}(g))$
  $= \lambda_{g_1}(g_2 g) = (g_1 g_2)g$
  $= \lambda_{g_1 g_2}$
- Let $\phi: G \to \{\lambda_g : g \in G\}$.
- $\phi(g_1) = \lambda_{g_1}$ is a bijection and

  $\phi(g_1 g_2) = \lambda_{g_1 g_2} = \lambda_{g_1} \circ \lambda_{g_2} = \phi(g_1)\phi(g_2)$
- So ϕ is an isomorphism.

example:

$\mathbb{Z}_4 = \{0, 1, 2, 3\} \cong \{(1), (13)(24), (1234), (1432)\}$

+	0	1	2	3	$\sigma \in S_4$
0	0	1	2	3	(1)
1	1	2	3	0	(1234)
2	2	3	0	1	(13)(24)
3	3	0	1	2	(1432)

example:

- $S_3 \cong H \le S_6$

		1	2	3	4	5	6	S_3 is isomorphic to
		(1)	(12)	(13)	(23)	(123)	(132)	$\sigma \in S_6$
1	(1)	(1)	(12)	(13)	(23)	(123)	(132)	(1)
2	(12)	(12)	(1)	(132)	(123)	(23)	(13)	(12)(36)(45)
3	(13)	(13)	(123)	(1)	(132)	(12)	(23)	(13)(25)(46)
4	(23)	(23)	(132)	(123)	(1)	(13)	(12)	(14)(26)(35)
5	(123)	(123)	(13)	(23)	(12)	(132)	(1)	(156)(234)
6	(132)	(132)	(23)	(12)	(13)	(1)	(123)	(165)(243)

- $S_3 \cong \{(1), (12)(36)(45), (13)(25)(46), (14)(26)(35), (156)(234), (165)(243)\}$

---

thm: external direct products

- Let G, H be groups. Then $G \times H$ is a group

  $(g_1, h_1) \circ (g_2, h_2) = (g_1 g_2, h_1 h_2)$

---

thm:

- If a and b are positive integers with $\gcd(a,b) = 1$, then

  $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{ab}$

  $\mathbb{Z}_2 \times \mathbb{Z}_2 \not\cong \mathbb{Z}_4$

  $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$

proof:

- Let $\phi: \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ where

  $\phi(n) = (n \bmod a, n \bmod b)$
- Claim: ϕ is an isomorphism.

① ϕ is 1-1: Suppose $\phi(n) = \phi(m)$

then $n \equiv m \bmod a \Rightarrow a \mid n-m$

$n \equiv m \bmod b \Rightarrow b \mid n-m$

So $n \equiv m \bmod (\operatorname{lcm}(a,b))$

$\Rightarrow n \equiv m \bmod ab$

So $n = m$ in $\mathbb{Z}_{ab}$.

② ϕ is onto: $|\mathbb{Z}_a \times \mathbb{Z}_b| = ab$

$|\mathbb{Z}_{ab}| = ab$.

Since $|\mathbb{Z}_a \times \mathbb{Z}_b| = |\mathbb{Z}_{ab}|$ and ϕ is 1-1, then ϕ is onto.

③ ϕ is a homomorphism: (is,1) $\phi(n+m) = \phi(n) + \phi(m)$

$\phi(n+m) = ((n+m) \bmod a, (n+m) \bmod b)$

$\phi(n) + \phi(m) = (n \bmod a, n \bmod b) + (m \bmod a, m \bmod b)$

$= ((n+m) \bmod a, (n+m) \bmod b)$

$= \phi(n+m)$

---

thm: internal direct product

- Let H and K be subgroups of G satisfying
  1. $G = HK = \{hk;\ h \in H, k \in K\}$
  2. $H \cap K = \{e\}$
  3. $hk = kh$ for all $h \in H$ and $k \in K$.

Then G is the internal direct product of H and K

Then $G \cong H \times K$.

example:

- $\{0,2,4\}, \{0,3\}$ in $\mathbb{Z}_6$
- $\{0,2,4\} + \{0,3\} = \{0+0, 0+3, 2+0, 2+3, 4+0, 4+3\}$

$= \{0, 3, 2, 5, 4, 1\}$

$= \mathbb{Z}_6$

example:

- $\mathbb{Z}_8^\times = \{1,3,5,7\}$
- $\{1,3\}\{1,5\} = \{1,5,3,7\} = \mathbb{Z}_8^\times$

example:

- D_6 is the internal product of $\{1, r^3\}$ and $\{1, r^2, r^4, s, r^2s, r^4s\}$
- Recall, in D_n, $r^i s = sr^{n-i}$. In D_6, $\boxed{r^3} = s^{r^{6-3}} = \boxed{sr^3}$

---

thm:

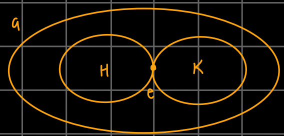
- If G is the internal direct product of H and K, then $G \cong H \times K$.

proof:

- $\phi: H \times K \to G$

$\phi(h,k) = hk \in G$

ϕ is well-defined.



- WTS: ϕ is onto
  - Let $g \in G$. Since $G = HK$, then $g = hk$ for some $h \in H$, $k \in K$.

    So $\phi((h,k)) = hk = g$.
- WTS: ϕ is 1-1
  - Suppose $\phi((h_1,k_1)) = \phi((h_2,k_2))$ then

    $h_1k_1 = h_2k_2 \Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\}$

    $h_2^{-1}h_1 = e$ and $k_2k_1^{-1} = e$

    so $h_1 = h_2$ and $k_1 = k_2$.
- WTS: ϕ is a homomorphism so $\phi((h_1,k_1)(h_2,k_2)) = \phi((h_1,k_1))\phi((h_2,k_2))$
  - $\phi((h_1,k_1))\phi((h_2,k_2)) = (h_1k_1)(h_2k_2)$

    $= h_1(k_1h_2)k_2 = h_1(h_2k_1)k_2$

    $= (h_1h_2)(k_1k_2) = \phi((h_1h_2, k_1k_2))$

    $= \phi((h_1k_1)(h_2k_2))$ ☒

---

subgroup of G

thm: normal subgroup

$gNg^{-1} = N \Rightarrow gng^{-1} = n'$ for $n, n' \in N$.

conjugating n by g results in n' (could be n)

- N is a normal subgroup of G if $N \leq G$ and $gN = Ng$ for all $g \in G$.
- We write $N \trianglelefteq G$.

---

thm: abelian subgroups are normal

- If G is an abelian group and $H \leq G$, then $H \trianglelefteq G$.

proof:

- $gH = Hg$ because G is commutative.

---

thm:

- If $H \leq G$ and $[G:H] = 2$ then $H \trianglelefteq G$.

proof:

- Let $g \notin H$, then the left cosets of H are H and gH,

  the right cosets are H and Hg.

  $\Rightarrow gH = Hg$.

---

thm:

- Let $N \leq G$. The following are equivalent.
  1. $N \trianglelefteq G$ — $gH = Hg\ \ \forall g \in G$
  2. $gNg^{-1} \subseteq N\ \ \forall g \in G$. — $gng^{-1} \in N$ → closure
  3. $gNg^{-1} = N\ \ \forall g \in G$.

right mult by g^{-1}

proof: (3) ⇒ (2) ⇒ (1) ⇒ (3)

- (3) ⇒ (2). $gNg^{-1} = N \Rightarrow gNg^{-1} \subseteq N$.
- (2) ⇒ (1). Let $g \in G$. WTS $gN = Ng$. We know $gNg^{-1} \subseteq N$.
  - Let $x \in Ng \Rightarrow x = gn$ for some $n \in N$.
    - Then $xg^{-1} = gng^{-1} \in N$. So $xg^{-1} = n' \in N$.
    - So $x = n'g \in Ng$. So $gN \subseteq Ng$.
  - Let $y \in Ng \Rightarrow y = ng$ for some $n \in N$.
    - Because G is a group, $g^{-1} \in G$ so $g^{-1}Ng \subseteq N$.
    - $g^{-1}y = g^{-1}ng \in N$. So $g^{-1}y = n' \in N$.
    - $y = gn' \in gN$. So $Ng \subseteq gN$.
  - Hence $gN = Ng$.
- (1) ⇒ (3) Let $g \in G$. WTS: $gNg^{-1} = N$.
  - Let $x = gNg^{-1} \Rightarrow x = gng^{-1} = (gn)g^{-1}$ for some $n \in N$.
  - $gn \in gN$ and $gN = Ng$ so $gn \in Ng$ so $\exists n'$ s.t. $gn = n'g$.
  - Let $y \in N$. Then $yg \in Ng \Rightarrow yg \in gN$.
  - So $yg = gn$ for some $n \in N$.

    $y = gng^{-1} \in gNg^{-1}$.
  - So $gNg^{-1} = N$.

definition: quotient / factor groups

- Suppose $N \trianglelefteq G$ then G/N is a group where the elements of G/N are the cosets of N in G and the operation is $(g_1N)(g_2N) = \underbrace{(g_1g_2)}_{\text{operation in } G}N$

"a mod N"

$\mathbb{Z}$

$\mathbb{Z}/5\mathbb{Z}$

- $5\mathbb{Z}$ subgroup
- $1+5\mathbb{Z}$
- $2+5\mathbb{Z}$
- $3+5\mathbb{Z}$
- $4+5\mathbb{Z}$

cosets

example:

- $\mathbb{Z}/5\mathbb{Z}$ $\quad 5\mathbb{Z} \leq \mathbb{Z}$ so $5\mathbb{Z} \trianglelefteq \mathbb{Z}$
- $\mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}\}$
- $(3+5\mathbb{Z}) + (2+5\mathbb{Z}) = (3+2) + 5\mathbb{Z} = 0 + 5\mathbb{Z}$

$$((3+5x)+5\mathbb{Z}) + ((2+5k)+5\mathbb{Z}) = ((5+5x+5k)+5\mathbb{Z})$$
$$= ((0+5a)+5\mathbb{Z})$$
$$= (0+5\mathbb{Z})$$

$\boxed{\text{well-defined}}$

proof:

1. closed: $(g_1N)(g_2N) = (g_1g_2)N \in G/N$.
2. assoc: $((g_1N)(g_2N))(g_3N) = ((g_1g_2)N)g_3N$
$$= ((g_1g_2)g_3)N$$
$$= (g_1(g_2g_3))N$$
$$= (g_1N)((g_2g_3)N)$$
$$= (g_1N)((g_2N)(g_3N))$$
3. identity: $eN = N$ where e is the identity of G.
$$(gN)(eN) = (ge)N = gN$$
$$(eN)(gN) = (eg)N = gN$$
4. inverses: $(gN)^{-1} = g^{-1}N$
$$(gN)(gN)^{-1} = (gg^{-1})N = eN$$
$$(g^{-1}N)(gN) = (g^{-1}g)N = eN$$

5. well defined:

given: $g_1N = g_1'N$ and $g_2N = g_2'N$

WWTS: $(g_1g_2)N = (g_1'g_2')N$

1. $g_1N = g_1'N$ [given]
   $g_2N = g_2'N$
2. $(g_1')^{-1}g_1N \in N$ [difference of cosets $\in N$]
   $(g_2')^{-1}g_2N \in N$
3. $g_1 = g_1'n_1$ [left multiply (2) by g_1']
   $g_2 = g_2'n_2$
4. $g_1g_2 = (g_1'n_1)(g_2'n_2)$
   $= g_1'(n_1g_2')n_2$ [associativity]
5. Since $N \trianglelefteq G$, we have $gNg^{-1} \in N$
   $\Rightarrow gng^{-1} = n'$
   $\Rightarrow gn = n'g$
   Let $n_1g_2' = g_2'n_3$ for $n' = n_1$ and $g = g_2'$
6. Then
$$g_1g_2 = g_1'(g_2'n_3)n_2$$
$$= (g_1'g_2')(n_3n_2)$$
$$= (g_1'g_2')n_4 \quad \text{[renaming]}$$
$$(g_1'g_2')^{-1}(g_1g_2) = n_4 \Rightarrow (g_1g_2)N = (g_1'g_2')N \quad \boxtimes$$

example:

- $\mathbb{R}[x]$ = set of polynomials with real coefficients.
- $\mathbb{R}[x]$ is a group under addition.
- $x^2+1 \in \mathbb{R}[x]$
- $H = \{(x^2+1)q(x) : q \in \mathbb{R}[x]\}$
- $\mathbb{R}[x]/H = ?$
- the cosets are of the form
$$f(x) + H$$
where $f(x) \in \mathbb{R}[x]$
- $x + H = x + H$
$$x^2 + H = (-1) + \underbrace{(x^2+1)}_{\in H} + H$$
$$= (-1) + H$$
- $\mathbb{R}[x]/H = \{(a+bx) + H \mid a, b \in \mathbb{R}\} \cong (\mathbb{C}, +)$

---

thm: the alternating group (A_n) is normal in S_n

- $A_n \trianglelefteq S_n$

proof:

- If $n=1$, $A_1 = S_n$.
- If $n \geq 2$, $|A_n| = \frac{|S_n|}{2}$
  so $[S_n : A_n] = 2 \Rightarrow A_n \trianglelefteq S_n$

$S_n/A_n = \{A_n, B_n\}$

	A_n	B_n
A_n	A_n	B_n
B_n	B_n	A_n

---

definition: simple group

- We say G is a simple group if $N \trianglelefteq G$
  $\Rightarrow N = \{e\}$ or $N = G$.

prime

---

thm: any prime sized group is simple

- If $|G| = p$ with p prime, then G is simple.

proof:

- $|G| = p$.
- $H \leq G \Rightarrow |H| \mid |G| = p$.
- so $|H| = 1$ or $|H| = p$
$$\Downarrow \qquad\qquad \Downarrow$$
$$H = \{e\} \qquad H = G$$

---

thm: A_4 is not simple

proof:

- $A_4 = \{(1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$
- $H = \{(1), (12)(34), (13)(24), (14)(23)\}$
- $(123)H = \{(123), (134), (243), (142)\} = H(123)$
- $(132)H = \{(132), (143), (234), (124)\} = H(132)$

thm: For $n \geq 5$, A_n is simple

proof:

step 1: prove A_n is generated by 3-cycles

example: $A_4 = \{(1), (123), (132), (124), (142), (134), (143),$
$(234), (243), (12)(34), (13)(24), (14)(23)\}$

- $(12)(34) = (132)(134)$
- $(13)(24) = (123)(124)$
- $(14)(23) = (124)(123)$
- $(ab)(cd) = (acb)(acd) \quad a \neq b \neq c \neq d.$

proof:

- $\sigma \in A_n$ can be written as a product of a even number of transitions. There are 3 cases:
  - ① $(ab)(ab) = (1)$
  - ② $(ab)(ac) = (acb)$
  - ③ $(ab)(cd) = (acb)(acd)$
- So σ can be written as a product (possibly empty) of 3-cycles.

step 2: Show that if $N \trianglelefteq A_n$ and N contains a 3-cycle then contain all 3-cycles for $n \geq 3$.

proof:

- Suppose $(abc) \in N$.
- Since $N \trianglelefteq A_n$, for any $\sigma \in A_n$

  $\sigma(abc)\sigma^{-1} \in N$

  $\Rightarrow (\sigma(a)\ \sigma(b)\ \sigma(c)) \in N.$
- Now we need σ s.t

  $\sigma(a) = i$; $\sigma(b) = j$; $\sigma(c) = k$.

step 3: If $N \trianglelefteq A_n$ and $N \neq \{(1)\}$ and $n \geq 5$. N contains a 3-cycle.

proof:

- Suppose $N \trianglelefteq A_n$, $n \geq 5$ and $N \neq \{(1)\}$.
- Let $\sigma \in N$.
- Write σ as a product of disjoint cycle.
- If σ has a divisor with cycle length ≥ 4, then

  $\sigma = \tau(a_1 a_2 \ldots a_r)$ with τ disjoint from $(a_1 a_2 \ldots a_r)$ and $r \geq 4$.
- Consider $(a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1} \in N$

  $(a_1 a_2 a_3)(\tau(a_1 a_2 \ldots a_r))(a_1 a_2 a_3)^{-1}$

  $= (a_1 a_2 a_3)\tau(a_1 a_2 a_3)^{-1}(a_1 a_2 a_3)(a_1 a_2 \ldots a_r)(a_1 a_2 a_3)^{-1}$

  $= \tau(a_2 a_3 a_1 a_4 \ldots a_r) \in N$

  $\sigma^{-1} \in N$ so

  $\sigma^{-1}\tau(a_2 a_3 a_1 a_4 \ldots a_r) \in N.$

  $(a_1 a_r a_{r-1} \ldots a_2)\tau^{-1}\tau(a_2 a_3 a_1 a_4 \ldots a_r)$

  $= (a_1 a_r a_{r-1} \ldots a_2)(a_2 a_3 a_4 \ldots a_r)$

  $= (a_1 a_3 a_r)(a_2)(a_4) \ldots (a_{r-1})$

  $= (a_1 a_3 a_r) \in N.$

- If σ does not have factors with cycles of 4 or more elements.
- Another case:

  $\sigma = \tau(a_1 a_2 a_3)(a_4 a_5 a_6) \qquad n \geq 6$

  $(a_1 a_2 a_4)\sigma(a_1 a_2 a_4)^{-1} \in N$

  so

  $\sigma(a_1 a_2 a_4)\sigma(a_1 a_2 a_4)^{-1} \in N$

  so

  $(a_4 a_6 a_5)(a_1 a_3 a_2)\cancel{\tau^{-1}}(a_1 a_2 a_4)\cancel{\tau}(a_1 a_2 a_3)(a_4 a_5 a_6)(a_1 a_2 a_4)^{-1} \in N$

  $= (a_1 a_4 a_2 a_6 a_3) \in N$

  Since $r \geq 4$, it must contain a 3-cycle.

- Now, suppose $\sigma = \tau(a_1 a_2 a_3)$ where τ is the product of an even number of disjoint transpositions.

  $\sigma^2 \in N$

  $\sigma^2 = \tau^2(a_1 a_3 a_2) = (a_1 a_3 a_2) \in N.$

  So N contains a 3-cycle.

- Now suppose $\sigma = \tau_1 \tau_2 \ldots \tau_{2k-1} \tau_{2k} \in N.$

  $= \tau(a_1 a_2)(a_3 a_4)$

  $= \tau(a_1 a_3 a_2)(a_1 a_3 a_4)$
- Consider $(a_1 a_2 a_3)\sigma(a_1 a_3 a_2) \in N.$

  $\sigma^{-1}(a_1 a_2 a_3)\sigma(a_1 a_3 a_2) \in N$

  $\cancel{\tau}(a_1 a_2)(a_3 a_4)(a_1 a_2 a_3)\cancel{\tau}(a_1 a_2)(a_3 a_4)(a_1 a_3 a_2)$

  $= (a_1 a_3)(a_2 a_4) \in N$
- $\exists b \neq 1, 2, 3, 4$
- Consider the cycle $\mu = (a_1 a_3 b) \in A_n$

  $\mu^{-1}(a_1 a_3)(a_2 a_4)\mu \in N$

  $\mu^{-1}(a_1 a_3)(a_2 a_4)\mu(a_1 a_3)(a_2 a_4) \in N$

  $= (a_1 a_3 b) \in N.$

proof of thm:

- Let $n \geq 5$.
- Suppose $N \trianglelefteq A_n$ and $N \neq \{(1)\}$.
- Then, by step 3, N contains a 3-cycle.
- Then, by step 2, N contains all 3-cycles.
- Then, by step 1, $N = A_n$.
- Therefore, the only normal subgroups of A_n are $N = \{(1)\}$ and $N = A_n$.
- Thus, A_n is simple for $n \geq 5$.

definition: group homomorphism

- Let G, H be groups, $\phi: G \to H$ is a group homomorphism if $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ for any $g_1, g_2 \in G$.

example: $\phi: \mathbb{Z}_5 \to \mathbb{Z}_{12}$

- Suppose ϕ is a homomorphism.
  - $\phi(0) = \phi(0+0) = \phi(0) + \phi(0)$
  - $\phi(1) = \phi(5) = \phi(4+1) = \phi(4) + \phi(1) = \phi(3) + \phi(1) + \phi(1) \dots$
    $= 5 \cdot \phi(1)$
    $\equiv 0 \bmod 12$
- $\Rightarrow \phi(1) = 0 \Rightarrow \phi(n) = 0 \quad \forall n$

example: $\phi: \mathbb{Z}_{12} \to \mathbb{Z}_5$

- $\phi(0) = 0$
- $\phi(0) = \phi(12) = 12\phi(1)$
  $\equiv 0 \bmod 5$
  $\phi(1) \in \{0, 5, 10\}$

example: $\phi: \mathbb{Z}_4 \to \mathbb{Z}_{12}$

- $\phi(0) = 0$
- $\phi(1) = \phi(4) = 4\phi(1)$
  $\equiv 0 \bmod 12$
  $\Rightarrow \phi(1) \equiv 0 \bmod 3$
  $\Rightarrow \phi(1) \in \{0, 3, 6, 9\}$

$\phi(0) = 0$	$\phi(0) = 0$	$\phi(0) = 0$	$\phi(0) = 0$
$\phi(1) = 0$	$\phi(1) = 3$	$\phi(1) = 6$	$\phi(1) = 9$
$\phi(2) = 0$	$\phi(2) = 6$	$\phi(2) = 0$	$\phi(2) = 6$
$\phi(3) = 0$	$\phi(3) = 9$	$\phi(3) = 0$	$\phi(3) = 3$
	$\leq \mathbb{Z}_{12}$		

example: $\phi: \mathbb{Z}_8 \to \mathbb{Z}_{12}$

- $\phi(0) = 0$
- $\phi(1) = k$
- $8k \equiv 0 \bmod 12$
  $2k \equiv 0 \bmod 3$
  $k \equiv 0 \bmod 3 \quad [\gcd(2,3) = 1]$
- $\Rightarrow \phi(1) \in \{0, 3, 6, 9\}$

		$\leq \mathbb{Z}_{12}$	
$\phi(0) = 0$	$\phi(0) = 0$	$\phi(0) = 0$	$\phi(0) = 0$
$\phi(1) = 0$	$\phi(1) = 3$	$\phi(1) = 6$	$\phi(1) = 9$
$\vdots$	$\phi(2) = 6$	$\phi(2) = 0$	$\phi(2) = 6$
$\vdots$	$\phi(3) = 9$	$\phi(3) = 6$	$\phi(3) = 3$
$\vdots$	$\phi(4) = 0$	$\vdots$	$\phi(4) = 0$
$\vdots$	$\phi(5) = 3$	$\vdots$	$\vdots$
$\vdots$	$\phi(6) = 6$	$\vdots$	$\vdots$
$\phi(7) = 0$	$\phi(7) = 9$	$\phi(7) = 6$	$\phi(7) = 3$

example: $\phi: \mathbb{Z}_m \to \mathbb{Z}_n$

- $\phi(0) = 0$
- generator $\phi(1) = k \Rightarrow \phi(\ell) = \ell k \bmod n$
  $km \equiv 0 \bmod n$
  $d = \gcd(m,n) \Rightarrow m = dm', n = dn'$
  $km' \equiv 0 \bmod n'$
  $k \equiv 0 \bmod n'$
- $\therefore k \in \{0, n', 2n', (d-1)n'\}$

The number of homomorphisms from $\mathbb{Z}_m$ to $\mathbb{Z}_n$ is $d = \gcd(m,n)$.

example: $\phi: \mathbb{Z}_m \to \mathbb{Z}$

- $km = 0 \Rightarrow k = 0$

example: $\phi: \mathbb{Z} \to \mathbb{Z}_m$

- $\phi(0) = 0$
- $\phi(1) = k \bmod m$
- $\Rightarrow k \in \{0, 1, \dots, m-1\}$

---

thm:

- Let G, H be groups and $\phi: G \to H$ be a group homomorphism.
- Then,
  1. let $\phi(G) = \{\phi(g) \mid g \in G\} = \mathrm{Im}(\phi) \leq H$.
  2. $\phi(e_G) = e_H$
  3. $\ker\phi = \{g \in G \mid \phi(g) = e_H\} \trianglelefteq G$.
  4. $G' \leq G$, $\phi(G') \leq H$

proof: 1. $\mathrm{Im}(\phi) \leq H$

- subset:
  - $x \in \phi(G) \Rightarrow x = \phi(g)$ for some $g \in G$. $x = \phi(g) \in H$.
- closed:
  - let $\phi(g_1) \in \phi G$ and $\phi(g_2) \in \phi G$
  - Then $\phi(g_1) \cdot \phi(g_2) = \phi(g_1 g_2) \in \phi(G)$
- identity:
  - $\phi(e_G) = e_H \in \phi(G)$.
- inverse:
  - let $\phi(g) \in \phi(G)$. $g^{-1} \in G$ so $\phi(g^{-1}) \in \phi(G)$
  - $\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(e_G) = e_H$
    $\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e_G) = e_H$

proof: ③ $\ker\phi \trianglelefteq G$

- subset:
  - $g \in \ker\phi \Rightarrow g \in G$ by definition.
- closed:
  - Let $g_1, g_2 \in \ker\phi$.

    Then $\phi(g_1) = e_H$ and $\phi(g_2) = e_H$

    $\Rightarrow \phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ [homomorphism]

    $= e_H$ [definition]
- identity:
  - $\phi(e_G) = e_H$ so $e_G \in \ker\phi$.
- inverses:
  - Let $g \in \ker\phi$
  - Since ϕ is a homomorphism,

    $\phi(g^{-1}) = \phi(g)^{-1} = e^{-1} = e \Rightarrow g^{-1} \in \ker\phi$.
- normality:
  - Let $g \in G$ and $k \in \ker\phi$.
  - WTS: $gkg^{-1} \in \ker\phi$
  - Consider $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1})$

    $= \phi(g)\phi(g^{-1})$ [$k \in \ker\phi \Rightarrow \phi(k) = e_H$]

    $= \phi(gg^{-1})$

    $= \phi(e_G) = e_H \in \ker\phi$ [G is a group]

---

thm: 1st isomorphism theorem (fundamental homomorphism theorem)

- Let $\phi: G \to H$ be a group homomorphism, Then

$$G/\ker\phi \cong \phi(G)$$

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\eta"'] & H \\ G/\ker\phi \arrow[ur, dashed, "\psi"'] & \end{tikzcd}$$

$\eta(g) = g\ker\phi$

example: $\phi: \mathbb{Z}_8 \to \mathbb{Z}_{12}$

- $\phi(m) = 3m \bmod 12$
- $\phi(\mathbb{Z}_8) = \{0,3,6,9\}$
- $\ker\phi = \{0,4\}$

$\phi(0) = 0$ $\quad \phi(4) = 0$

$\phi(1) = 3$ $\quad \phi(5) = 3$

$\phi(2) = 6$ $\quad \phi(6) = 6$

$\phi(3) = 9$ $\quad \phi(7) = 9$

- $\mathbb{Z}_8/\{0,4\} \cong \underbrace{\{0,3,6,9\}}_{= \langle 3\rangle} \leq \mathbb{Z}_{12}$

  $= \{\{0,4\},\{1,5\},\{2,6\},\{3,7\}\}$

proof:

- $$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\eta"'] & H \\ G/\ker\phi \arrow[ur, dashed, "\psi"'] & \end{tikzcd}$$

  If $\phi: G \to H$, Then $G/\ker\phi \cong \phi(G) = H$

- Let $\eta: G \to G/\ker\phi$ where $\eta(g) = g(\ker\phi)$
- Let $\psi: G/\ker\phi \to \phi(G)$ where $\psi(g\ker\phi) = \phi(g)$
- If $g\ker\phi \in G/\ker\phi \Rightarrow \psi(g\ker\phi) \in \phi(G)$
- WTS:

  ① ψ is well defined (i.e. if $g_1\ker\phi = g_2\ker\phi$

  then $\psi(g_1\ker\phi) = \psi(g_2\ker\phi)$

  $\Rightarrow \phi(g_1) = \phi(g_2)$)

  ② ψ is 1-1

  ③ ψ is onto

  ④ ψ is a homomorphism

① Suppose $g_1\ker\phi = g_2\ker\phi$. WTS $\phi(g_1) = \phi(g_2)$.

$g_1\ker\phi = g_2\ker\phi \Rightarrow g_2^{-1}g_1 \in \ker\phi$

so $\phi(g_2^{-1}g_1) = e$ [kernel definition]

$\Rightarrow \phi(g_2^{-1})\phi(g_1) = e$ [ϕ is an isomorphism]

$\phi(g_2)\phi(g_2^{-1})\phi(g_1) = \phi(g_2)$ [left-multiply by $\phi(g_2)$]

$\phi(g_2g_2^{-1})\phi(g_1) = \phi(g_2)$ [ϕ is an isomorphism]

$\Rightarrow \phi(g_1) = \phi(g_2)$ [$\phi(g_2g_2^{-1}) = \phi(e) = e$]

② Suppose $\psi(g_1\ker\phi) = \psi(g_2\ker\phi)$

then $\phi(g_1) = \phi(g_2)$ [ψ definition]

so $\phi(g_2^{-1})(\phi(g_1)) = e$ [left multiply by $\phi(g_2^{-1})$]

$\phi(g_2^{-1}g_1) = e$ [ϕ is an isomorphism]

$\Rightarrow g_2^{-1}g_1 \in \ker\phi$ [$\ker\phi$ definition]

So $g_1\ker\theta = g_2\ker\phi$ [definition]

So ψ is 1-1.

③ Let $x \in \phi(G) \Rightarrow \exists g \in G$ s.t. $x = \phi(g)$.

$x = \phi(g) = \psi(g\ker\phi)$ [definition]

$\Rightarrow x \in \mathrm{Im}(\psi)$

So ψ is onto

④ $\psi((g_1\ker\phi)(g_2\ker\phi)) = \psi((g_1g_2)\ker\phi)$

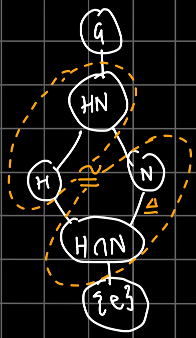
$= \phi(g_1g_2)$

$= \phi(g_1)\phi(g_2)$

$= \psi(g_1\ker\phi)\psi(g_2\ker\phi)$

thm: 2^{nd} isomorphism theorem

- Let $H \leq G$
- Let $N \trianglelefteq G$
- Then, (1) $HN \leq G$
  (2) $H \cap N \trianglelefteq H$
  (3) $H/H\cap N \cong HN/N$



example:

- $D_4 = \{(1), (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\}$
- $H = \{1, s\} \leq D_4$
- $N = \{1, r^2, s, r^2 s\} \trianglelefteq D_4$
- $HN = \{hn \mid h \in H, n \in N\}$
  $= \{1, r^2, s, r^2 s\} = N$
  $H \subseteq HN$ and $N \subseteq HN$ since $1 \in HN$
- $H \cap N = \{1, s\} \trianglelefteq \{1, s\}$
- $H/H\cap N = \{1,s\}/\{1,s\} = \{\{1,s\}\}$
- $HN/N = \{1, r^2, s, r^2, r^2 s\}/\{1, r^2, s, r^2, r^2 s\} = \{\{1, r^2, s, r^2, r^2 s\}\}$

proof: (1) $HN \leq G$.

- Recall, $HN = \{hn \mid h \in H, n \in N\}$
  - identity: $e \in H$ and $e \in N$ because $H, N \leq G$.
    so $e \cdot e = e \cdot e = e \in HN$.
  - subset: $h \in G, n \in G$ so $hn \in G$.
  - closed: Let $h_1 n_1 \in HN$, $h_2 n_2 \in HN$.
    $(h_1 n_1)(h_2 n_2) = h_1 (n_1 h_2) n_2$
    $= h_1 (h_2 n_1') n_2$ $[N \trianglelefteq G]$
    $= h_1 h_2 (n_1' n_2)$
    $= h_3 n_3 \in HN$
  - inverse: Let $hn \in HN$.
    $(hn)^{-1} = n^{-1} h^{-1}$
    $= h^{-1} (n')^{-1} \in HN$ $[N \trianglelefteq G]$

proof: (2) $H \cap N \trianglelefteq G$

- $H \cap N \subseteq H$.
- Since $H \cap N$ is a group with the same operator as H, then $H \cap N \leq H$.
- Let $h \in H$, $k \in H \cap N$ WTS $hkh^{-1} \in H \cap N$.
- $k \in H \cap N \Rightarrow k \in H$
- $\Rightarrow hkh^{-1} \in H$ (H is closed).
- similar, $k \in H \cap N \Rightarrow k \in N$
- Since $N \trianglelefteq G$, $hkh^{-1} \in N$.
- So, $hkh^{-1} \in H \cap N \Rightarrow H \cap N \trianglelefteq G$

proof: (3) $H/H\cap N \cong HN/N$.

- First, let's show that $N \trianglelefteq HN$.
- WTS: $xNx^{-1} \in N$ for some $x \in HN$.
- $N \trianglelefteq G \Rightarrow gNg^{-1} = N$
- Now, let $x \in HN \subseteq G$. Then $xNx^{-1} \in N$.
- Hence $N \trianglelefteq HN$.
- So $N \trianglelefteq HN$.
  we want to invoke the 1st iso thm s.t. $H \cap N = \ker\phi$ and $HN/N = \operatorname{Im}\phi$
- Now, define $\phi: H \to HN/N$ by $\phi(h) = hN$.
- claim: ϕ is a well-defined homomorphism.
- well defined: WTS $hN \in HN/N$.
- $HN = \{hn \mid h \in H, n \in N\}$
- $HN/N = \{hnN \mid h \in H, n \in N\} = \{hN \mid h \in H\}$
- So $hN \in HN/N$.
- onto: Let $x \in HN/N$.
- Then $x = (hn)N = hN = \phi(h)$ for some $h \in H$, $n \in N$.
- isomorphism:
- $\phi(h_1 h_2) = (h_1 h_2)N$
  $= (h_1 N)(h_2 N)$ $[N \trianglelefteq HN]$
  $= \phi(h_1)\phi(h_2)$
- So ϕ is a homomorphism.
- By the 1st isomorphism theorem,
- $H/\ker\phi \cong \phi(H) = HN/N$
- Claim: $\ker\phi = H \cap N$
  N is the identity element of HN/N
- $\ker\phi = \{h \in H \mid \phi(h) = N\} = \{h \in H \mid hN = N\} = H \cap N$
- So,
  $$H/H\cap N \cong HN/N$$

example:

- $G = \mathbb{Z}$
- $H = m\mathbb{Z}$
- $N = n\mathbb{Z}$
- $H \cap N = \operatorname{lcm}(m,n)\mathbb{Z}$
- $HN = m\mathbb{Z} + n\mathbb{Z} = \gcd(m,n)\mathbb{Z}$
- $H/H\cap N \cong HN/N$
  $m\mathbb{Z}/\operatorname{lcm}(m,n)\mathbb{Z} \cong \gcd(m,n)\mathbb{Z}/n\mathbb{Z}$
- So $|m\mathbb{Z}/\operatorname{lcm}(m,n)\mathbb{Z}| = |\gcd(m,n)\mathbb{Z}/n\mathbb{Z}|$
  $\operatorname{lcm}(m,n)/n = n/\gcd(m,n)$
  $\Rightarrow mn = \operatorname{lcm}(m,n) \cdot \gcd(m,n)$

4th isomorphism theorem

thm: correspondence theorem

- $N \trianglelefteq G$ maps $H \to H/N$ is a 1-1 correspondence between subgroups $H \leq G$ containing N and the set of subgroups of G/N.
- Furthermore, $H \trianglelefteq G$ and $N \subseteq H$ then $H/N \trianglelefteq G/N$.

① If $N \trianglelefteq G$, then $H/N \leq G/N$
$N \subseteq H \subseteq G$

② if $H \trianglelefteq G$ then $H/N \trianglelefteq G/N$

③ if $H/N \leq G/N$ then $H \leq G$ with $N \subseteq H$

④ if $H/N \trianglelefteq G/N$ then $H \trianglelefteq G$ with $N \subseteq H$

proof: ① $N \trianglelefteq G$, $N \subseteq H \subseteq G \Rightarrow H/N \leq G/N$

- N, G, H are all groups with the same operation.
- $N \trianglelefteq G \Rightarrow gng^{-1} \in N$.
- $H \leq G \Rightarrow n \in h \Rightarrow h \in G$.
- so $nnh^{-1} \in N$ so $N \trianglelefteq G$.
- H/N is a group (same operation as G/N).
- $(h_1N)(h_2N) = (h_1h_2)N$
  $= gN$
- so $H/N \subseteq G/N \Rightarrow H/N \leq G/N$

proof: ② $H \trianglelefteq G \Rightarrow H/N \trianglelefteq G/N$

- Let $gN \in G/N$ and $hN \in H/N$
- then, $(gN)(hN)(gN)^{-1}$
  $= (gN)(hN(g^{-1}N))$
  $= (ghg^{-1})N$
- $H \trianglelefteq G \Rightarrow ghg^{-1} \in H$
- so $(ghg^{-1})N \in H/N$
  $\Rightarrow (gN)(hN)(gN)^{-1} \in H/N \Rightarrow H/N \trianglelefteq G/N$

proof: ③ $H/N \leq G/N \Rightarrow H \leq G$, $N \subseteq H \subseteq G$

thm: 3rd isomorphism theorem

- Let G be a group.
- Let $N \subseteq H$, $N \trianglelefteq G$, $H \trianglelefteq G$.
- Then,
$$G/H \cong {G/N}\big/{H/N}$$

proof:

- Let $\phi : G/N \to G/H$
  $\phi(gN) = gH$
- $\ker\phi = \{gN \in G/N \mid gH = H\}$
  $= H/N$
- By the 1st isomorphism theorem,
  $G/N / H/N \cong G/H$

---

definition: group actions

- A group G acts on a set X with a group action if there is a binary action from
$$G \times X \to X$$
such that
  1) $e \cdot x = x \quad \forall x \in X$
  2) $(g_1g_2)\cdot x = g_1\cdot(g_2\cdot x) \quad \forall g_1, g_2 \in G, \forall x \in X$.

- If a group action exists, we say X is a G-set.

example: trivial group action

- The trivial group action of G on X is the one defined by
$$g \cdot x = x \quad \forall g \in G, x \in X$$

  1) $e \in G$ so $e \cdot x = x$
  2) $(g_1g_2)\cdot x = x$
     $g_2 \cdot x = x$
     $g_1 \cdot x = x$
  so $g_1\cdot(g_2\cdot x) = g_1 \cdot x = x = (g_1g_2)\cdot x$

example: $G = D_4$ on $X = \{1,2,3,4\}$

- Let $\sigma \in D_4$ and define $\sigma \cdot x = \sigma(x)$.
- $D_4 = \{(1), (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\}$
- $(1234)\cdot 3 = 4$
- $(14)(23)\cdot 3 = 2$
- Let's prove it's a group action.
  1. $(1)\cdot x = x \quad \forall x \in X$
  2. Let $\sigma, \mu \in D_4$
     WTS: $\sigma\mu \cdot x = \sigma\cdot(\mu\cdot x)$
     $(\sigma\mu)\cdot x = \sigma(\mu(x))$
     $= \sigma(\mu \cdot x)$
     $= \sigma\cdot(\mu\cdot x)$ ⊠

definition: G-equivalence

- Let $x,y \in X$. We say $x \underset{G}{\sim} y$.
- If $\exists g \in G$ such that $g \cdot x = y$.
- In this case we say x and y are G-equivalent.

---

thm:

- $\sim_G$ describes an equivalence relation on set X.

proof:

- reflexive: Let $x \in X$. WTS $x \sim_G x$.
  $e \cdot x = x$, so $x \sim_G x$.
- symmetric: Let $x,y \in X$ s.t. $x \sim_G y$. WTS $y \sim_G x$.
  $x \sim_G y \Rightarrow g \cdot x = y$
  $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot y$
  $(g^{-1} g) \cdot x = g^{-1} \cdot y$
  $x = g^{-1} \cdot y$
  $\Rightarrow y \sim_G x$.
- transitive: Let $x,y,z \in X$ s.t. $x \sim_G y$, $y \sim_G z$ WTS $x \sim_G z$.
  $x \sim_G y \Rightarrow g_1 \cdot x = y$ for some $g_1 \in G$.
  $y \sim_G z \Rightarrow g_2 \cdot y = z$ for some $g_2 \in G$.
  Substituting, $g_2 \cdot (g_1 \cdot x) = z$
  $(g_2 g_1) \cdot x = z$
  $\Rightarrow x \sim_G z$.
- So $\sim_G$ describes an equivalence relation on set X. ⊠

---

definition: orbit of x

- Suppose G acts on X. Then,
  $[x] = \{g \cdot x \mid g \in G\}$

  fix an x and see where it gets sent to

  partitions X
- This is the orbit of x denoted by O_x.
  $O_x = \{g \cdot x \mid g \in G\}$

---

definition: fixed point set of G.

- This is defined as
  $X_g = \{x \in X \mid g \cdot x = x\}$

example:

- $X = \{1,2,3,4\}$
- $D_4 = \{(1),(1234),(13)(24),(1432),$
  $(12)(34),(14)(23),(13),(24)\}$
- $X_{(1)} = \{1,2,3,4\}$
- $X_{(13)} = \{2,4\}$
- $X_{(24)} = \{1,3\}$
- $X_{(12)(34)} = \emptyset = X_{(13)(24)} = X_{(14)(23)} = X_{(1234)} = X_{(1432)}$

what stays fixed?

definition: stabilizer (isotropic) subgroup of x

- This is defined as
  $G_x = \{g \in G \mid g \cdot x = x\} \leq G$

example:

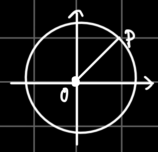
- $X = \{1,2,3,4\}$
- $D_4 = \{(1),(1234),(13)(24),(1432),$
  $(12)(34),(14)(23),(13),(24)\}$
- $G(1) = \{(1),(24)\}$
- $G(2) = \{(1),(13)\}$
- $G(3) = \{(1),(24)\}$
- $G(4) = \{(1),(13)\}$

which permutations fix

---

example:

- $G = (\mathbb{R},+)$ acting on $\mathbb{R}^2$
- $\theta \cdot (x,y) =$ rotation of (x,y) by θ radians
- $O_P =$ circle centered at the origin with radius $\overline{OP}$.



- $G_P = \{\theta \in \mathbb{R} \mid \theta \cdot P = P\}$
  $=$ which angles leave the point intact?
  $= \{2k\pi \mid k \in \mathbb{Z}\} = \langle 2\pi \rangle$

---

thm: G_x is a subgroup of G.

proof:

- $G_x \subseteq G$ by definition.
- Since $e \cdot x = x$, $e \in G_x$.
- Let $g,h \in G_x$. WTS: $gh \in G_x$. $g^{-1} \in G_x$.
- $g,h \in G_x \Rightarrow g \cdot x = h \cdot x = x$
  $\Rightarrow (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$
  $\Rightarrow gh \in G_x$.
- $e \cdot x = x \Rightarrow (g^{-1} g) \cdot x = x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x = x$
  $\Rightarrow g^{-1} \in G_x$.
- Thus, $G_x \leq G$ ⊠

thm:

- Let G be a finite group and X is a finite G-set. Then,
$$[G : G_x] = \theta_x$$
for any $x \in X$.

example:

- $X = \{1,2,3,4,5,6\}$
- $G = \{(1), (12)(3456), (35)(46), (12)(3654)\}$
- $G_1 = \{(1), (35)(46)\}$
- Now cosets of G_1 in G
  1. $G_1 = \{(1), (35)(46)\}$
  2. $(12)(3456)G_1 = \{(12)(3456), (12)(3654)\}$
- $\theta_1 = \{1, 2\}$

---

example:

- $X = \{1,2,3,4\}$
- $G = D_4$
- $G_1 = \{\sigma \in D_4 \mid \sigma(1) = 1\} = \{(1), (24)\}$
- Cosets:

1. $(1)G_1 = \{(1), (24)\}$	$\sigma(1) = 1$
2. $(13)G_1 = \{(13), (13)(24)\}$	$\sigma(1) = 3$
3. $(1234)G_1 = \{(1234), (12)(34)\}$	$\sigma(1) = 2$
4. $(1432)G_1 = \{(1432), (14)(23)\}$	$\sigma(1) = 4$

proof:

- Consider the coset hG_x.
- Now let $g \in hG_x \Rightarrow g = hk$ for some $k \in G_x$
- Then,
$$g \cdot x = (hk) \cdot x$$
$$= h \cdot (k \cdot x) \quad [\text{group action}]$$
$$= h \cdot x$$
- So, for any hG_x, we have $g \cdot x = h \cdot x$.
- Now suppose $h_1 G_x \neq h_2 G_x$. WTS $h_1 \cdot x \neq h_2 \cdot g$.
- FTSOC, suppose
$$h_1 \cdot x = h_2 \cdot x$$
$$\Rightarrow h_2^{-1} h_1 \cdot x = x$$
$$\Rightarrow h_2^{-1} h_1 \in G_x$$
$$\Rightarrow h_1 G_x = h_2 G_x \quad !$$
- Thus, $|G : G_x| \leq |\theta_x|$.
- Now, let $g \cdot x \in \theta_x$. Then
$$\ell \in gG_x$$
$$\Rightarrow \ell \cdot x = g \cdot x$$
- So, $|\theta_x| \leq [G : G_x]$.
- Thus, $|G : G_x| = |\theta_x|$.

- G acts on X.
- The orbits partition X.
- Suppose X is finite, choose $x_1, x_2, \dots, x_n$ to be the reps of each disjoint orbit. Then,
$$X = \bigcup_{i=1}^{n} \theta_{x_i} = |X| = |\theta_{x_1}| + |\theta_{x_2}| + \dots |\theta_{x_n}|$$
$$= (|\theta_{x_1}| + \dots + |\theta_{x_k}|) + \sum_{i=k+1}^{n} |\theta_{x_i}|$$
$$= |X_G| + \sum_{i=k+1}^{n} |\theta_{x_i}|$$

- $x \in \theta_x$ if $\theta_x = \{x\}$, then $g \cdot x = x \ \forall g \in G$.
- Suppose $x_1, x_2, \dots, x_k$ are the elements of X_G. Then,
$$\theta_{x_i} = \{x_i\} \text{ for } i = 1, 2, \dots, k$$
and $|\theta_{x_i}| > 1$ for $i = k+1, \dots, n$.
- Consider the group action where G acts on G by conjugation
$$g \cdot x = gxg^{-1}.$$
- The set of fixed points.
$$\{x \in G \mid gxg^{-1} = x \quad \forall g \in G\}$$
$$\{x \in G \mid gx = xg \quad \forall g \in G\}$$
$$= Z(G)$$
- Note,
$$|G| = |Z(G)| + \sum_{i=k+1}^{n} |\theta_{x_i}|$$
$$= |Z(G)| + \sum_{i=k+1}^{n} [G : G_{x_i}]$$

- Note,
$$G_{x_i} = \{g \in G \mid g \cdot x_i = x_i\}$$
$$= \{g \in G \mid g x_i g^{-1} = x_i\}$$
$$= \{g \in G \mid g x_i = x_i g\} = C(x_i)$$
centralizer subgroup of x_i

- This gives us the class equation:
$$|G| = |Z(G)| + \sum_{i=k+1}^{n} [G : C(x_i)]$$

- By definition, $|C(x_i)| < |G|$.
- If $|C(x_i)| = 1 \Rightarrow |\theta_{x_i}| = |G|$
- But $|Z(G)| \geq 1$ so $1 < |C(x_i)| < |G|$.
- Suppose $|G| = p^2$ and G is not abelian. Then, since $Z(G) \leq G$ and has group order that has to divide $|G|$,
$$|Z(G)| \in \{1, p\}$$
- Suppose $|Z(G)| = 1$, then
$$p^2 = 1 + \sum_{i=k+1}^{n} [G : C(x_i)]$$
divisors of p^2, none of which is 1.
$$p^2 = 1 + mp \quad !$$
- So $|Z(G)| = p$.

---

lemma: $Z(G) \trianglelefteq G$.

proof:

- $Z(G) \subseteq G$ by definition.
- $e \in Z(G)$ because $ge = eg = g$ $\forall g \in G$.
- Let $g_1, g_2 \in Z(G)$ and let $g \in G$.

$$\begin{aligned} \Rightarrow (g_1 g_2) g &= g_1 (g_2 g) && [\text{associativity}] \\ &= g_1 (g g_2) && [g_2 \in Z(G)] \\ &= (g_1 g) g_2 && [\text{associativity}] \\ &= (g g_1) g_2 && [g_1 \in Z(G)] \\ &= g (g_1 g_2) && [\text{associativity}]. \end{aligned}$$

- so $g_1 g_2 \in Z(G)$.
- Now let $g \in Z(G)$ and $h \in G$. WTS $hg^{-1} = g^{-1}h$.

$$\begin{aligned} (g^{-1}h)^{-1} &= h^{-1} g \\ &= g h^{-1} && [g \in Z(G)] \\ &= (hg^{-1})^{-1} \end{aligned}$$

- so $g^{-1}h = hg^{-1} \Rightarrow g^{-1} \in Z(G)$

alternative proof:

- Let $g \in G$ and $z \in Z(G)$. Then

$$\begin{aligned} g(zg^{-1}) &= g(g^{-1}z) && [z \in Z(G)] \\ &= (gg^{-1})z && [\text{associativity}] \\ &= z \in Z(G) && [\text{identity}] \end{aligned}$$

- Thus $Z(G) \trianglelefteq G$.

- $G/Z(G)$ is a group.
- $|G/Z(G)| = p$ so it's cyclic.
- Let $G/Z(G) = \langle a\, Z(G) \rangle$, then

$g Z(G) = a^m Z(G)$ for some m.

$\Rightarrow g = a^m x$ for some $x \in Z(G)$.

- $h = a^n y$ for some $n \in \mathbb{Z}$ and $y \in Z(G)$.
- $$\begin{aligned} gh &= (a^m x)(a^n y) \\ &= a^m (x a^n) y \\ &= a^m (a^n x) y && [x \in Z(G)] \\ &= a^{m+n} xy && [\text{associativity}] \\ hg &= (a^n y)(a^m x) \\ &= a^n (y a^m) x \\ &= a^n (a^m y) x \\ &= a^{m+n} yx \\ &= a^{m+n} xy \end{aligned}$$
- $gh = hg \Rightarrow G$ is abelian.

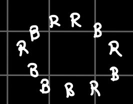
---

problem:

- Count how many necklaces with 11 beads can be created if each bead is red, white or blue.

solution.

- There are 3^{11} ways of placing 11 beads of one of 3 colors, but some of them will be repeated.



- $\mathbb{Z}_{11}$ acts on the coloring by rotation.

$i \cdot c$ = rotate coloring c by i clockwise

- $|\theta_c| = 11$.
- answer: $3 + \dfrac{3^{11} - 3}{11}$

---

thm: Burnside's theorem

- Let G be a finite group acting on a set X.
- Let k be the # of orbits of X. Then,

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

example: beads

- $G = \mathbb{Z}_{11} \Rightarrow |G| = 11$
- X = # colorings $\Rightarrow |X| = 3^{11}$
- $X_g = \{x \in X \mid g \cdot x = x\}$

$$\left.\begin{aligned} &|X_e| = |X| = 3^{11} \\ &|X_1| = 3 \\ &|X_2| = 3 \\ &\quad\vdots \\ &|X_{10}| = 3 \end{aligned}\right\} \Rightarrow k = \frac{1}{11}\left(3^{11} + 10 \cdot 3\right)$$

---

definition: ring

→ A non empty set R is a ring if it has two closed operations, addition and multiplication, satisfying the following conditions.

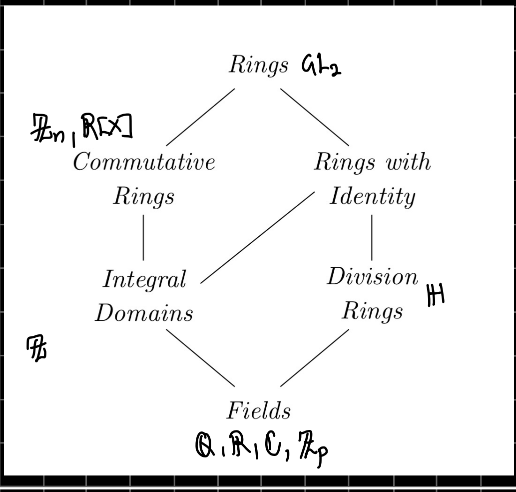
1. $a + b = b + a$ $\forall a, b \in R$ + commutativity
2. $(a+b)+c = a+(b+c)$ $\forall a,b,c \in R$ + associativity
3. $\exists 0 \in R$ s.t $a + 0 = a$ $\forall a \in R$ + identity
4. $\forall a \in R$, $\exists -a \in R$ s.t $a + (-a) = 0$ + inverse
5. $(ab)c = a(bc)$ $\forall a,b,c \in R$ × associativity
6. $\forall a,b,c \in R$ distribution

$a(b+c) = ab + ac$

$(a+b)c = ac + bc$

definition: types of rings

- If $\exists 1 \in R$ s.t $1 \neq 0$ and $1a = a1 = a \ \forall a \in R$, we say R is a ring with unity or identity.
- A ring R for which $ab = ba \ \forall a,b \in R$ is called a commutative ring.
- A commutative ring with identity is called an integral domain if $\forall a,b \in R$ s.t $ab = 0 \Rightarrow a = 0$ or $b = 0$.
- A division ring is a ring R, with identity, in which every nonzero element in R is a unit; that is, $\forall a \in R$ with $a \neq 0$, $\exists a^{-1}$ st $a^{-1}a = aa^{-1} = 1$.
- A commutative division ring is called a field.



---

thm:

→ If n is prime then $\mathbb{Z}_n$ is an integral domain.

proof:

- First, note that $\forall n \in \mathbb{Z}$, $\mathbb{Z}_n$ is a commutative ring. So, to prove it's an integral domain, we just need to show it has no zero divisors.
- Now, let p be a prime and let $x, y \in \mathbb{Z}_p$
- Consider $xy \equiv 0 \mod p$

  $\Rightarrow p \mid x$ or $p \mid y$.
- Since p is a prime, this implies

  $x \equiv 0 \mod p$ or $y \equiv 0 \mod y$
- Thus, $[x][y] = 0 \Rightarrow [x] = 0$ or $[y] = 0$.
- Thus, $\mathbb{Z}_p$ is an integral domain.

---

thm: fundamental proof of finite fields

→ If $\mathbb{F}$ is a finite field, then

$$|\mathbb{F}| = p^k \text{ for some } p, k \geq 1.$$

---

proposition:

- Let R be a ring with $a, b \in R$. Then
  1. $a0 = 0a = 0$
  2. $a(-b) = (-a)b = -ab$
  3. $(-a)(-b) = ab$

proof:

1. $a0 = a(0+0)$

   $= a0 + a0$

   $\cancel{a0 + (-a0)} = a0 + \cancel{a0 + (-a0)}$

   $0 = a0$

2. $ab + a(-b) = a(b-b)$

   $= a0$

   $= 0$

   $\Rightarrow a(-b) = -ab$

3. $(-a)(-b) = -(a(-b))$

   $= -(-ab)$

   $= ab$ $\square$

---

thm:

- Let D be a finite integral domain. Then D is a field.

proof:

- Let $a \in D$ with $a \neq 0$. WTS $\exists a^{-1}$ s.t $a^{-1}a = aa^{-1} = 1$.
- Consider the map $f: D \Rightarrow D$, $f(x) = ax$ (left-multiplication by a).
- We claim f is injective.

  Suppose $f(x_1) = f(x_2)$. Then

  $ax_1 = ax_2$

  $\Rightarrow a(x_1 - x_2) = 0$ $[\exists ax_2^{-1}$ and distributivity$]$

  $\Rightarrow x_1 - x_2 = 0$

  $\Rightarrow x_1 = x_2$

  in a finite algebraic structure injectivity forces surjectivity which often gives existence of inverses or solutions.

  So f is injective.
- Since D is finite, injectivity forces surjectivity.
- Since we have surjectivity, $\exists x \in D$ s.t

  $f(x) = ax = 1$
- Thus, this x is the multiplicative inverse of a.
- Since $\forall a \neq 0 \in D$, D is a field. $\square$

$\phi : G_1 \to G_2$ $\Rightarrow gH = Hg$

$H_1 \trianglelefteq G_1$

$\phi(H_1) = H_2$

$G_1/H_1 \cong G_2 H_2$

$\phi(gH_1) = gH_2$